Envoyé en préfecture le 26/05/2025
Reçu en préfecture le 26/05/2025
Publié le
ID : 069-256910183-20250523-CS_2025_05_4-DE

Syndicat Intercommunal des Technologies de l'Information pour les Villes

EXTRAIT DU REGISTRE DES DÉLIBÉRATIONS DU COMITÉ SYNDICAL

Séance du vendredi 23 mai 2025

N° CS_2025_05_4
Objet **: CONVENTION DE PARTENARIAT AVEC LA DIRECTION GENERALE DES FINANCES PUBLIQUES EN VUE DE L'EXPOSITION DE DOCUMENTS DE REMUNERATION SUR LE PORTAIL ENSAP**
Date de convocation **: lundi 12 mai 2025**
Date d'affichage du compte-rendu complet **: lundi 26 mai 2025**

Président de séance : Monsieur MILLET Pierre-Alain

Étaient présents (Titulaire(s) ou Suppléant(e)s) :

Monsieur MILLET Pierre-Alain,Monsieur VIOLLET Alain,Monsieur ARIAGNO Jeff,Monsieur DUGUA Axel,Monsieur MERMOURI Azdine,Monsieur SOW Abdoulaye,Madame VILLEDIEU Florence

Étaient absents ou excusés et ayant donné pouvoir (Titulaires ou Suppléants) :

Monsieur MAILLET Eric (donnant pouvoir à Monsieur VIOLLET Alain)

Étaient absents ou excusés :

Monsieur GUICHARD Rhida,Monsieur MOULIN Guillaume,Monsieur BONY Vincent,Monsieur RAPP Florian,Monsieur BON Gaël,Monsieur ELIEN Thierry

---

Déjà instituée pour les personnels civils de l'État, des magistrats et des militaires, la mise à disposition sous forme électronique des bulletins de paie ou de solde par le décret n° 2016-1073 du 3 août 2016 est étendue à l'ensemble des agents publics par le décret n° 2021-1752 du 21 décembre 2021 relatif aux modalités d'utilisation par certaines personnes morales de droit public de l'espace numérique sécurisé des agents publics et modifiant la durée de conservation des données au sein de ce traitement.
Ce décret prévoit l'application aux personnels des établissements publics de l'État, du Conseil constitutionnel, des groupements nationaux d'intérêt public, des collectivités locales, des établissements publics de santé, des établissements et services publics sociaux et médico-sociaux, des établissements publics locaux, des modalités de communication et de conservation sur support électronique des bulletins de paye et de solde en vigueur pour les agents de l'État,.

Il précise en outre que la conservation de ces documents par la direction générale des finances publiques s'opère pendant toute la carrière de l'agent et jusqu'à ce que celui-ci atteigne l'âge de soixante-quinze ans. L'ensembles des agents seront désormais informé par courriel de la mise à disposition de leur bulletin de paie sur l'espace numérique sécurisé de l'agent public (ensap ; https://ensap.gouv.fr/web/accueilnonconnecte).

LE COMITÉ SYNDICAL, APRÈS EN AVOIR DÉLIBÉRÉ,

A L'UNANIMITÉ DES SUFFRAGES EXPRIMÉS AVEC :

Envoyé en préfecture le 26/05/2025
Reçu en préfecture le 26/05/2025
Publié le
ID : 069-256910183-20250523-CS_2025_05_4-DE

8 VOIX POUR

DÉCIDE

- D'autoriser le traitement dématérialisé des bulletins de paie des agents dans les termes prévus par le décret 2016-1073 modifié par le décret 2021-1752.
-
- D'autoriser la signature de la convention d'éditeur-tiers de télétransmission avec la direction générale des finances publiques afin de proposer ce traitement à ses villes membres, ci-annexée.

- D'autoriser la signature de la convention d'employeur-émetteur avec la direction générale des finances publiques, ci-annexée.

Ainsi fait et délibéré les jours, mois et an susdits et ont signé les membres présents.

Pour expédition certifiée conforme,

Pierre Alain MILLET
Présidence du SITIV
26 mai 2025

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Légifrance
Le service public de la diffusion du droit

Décret n° 2016-1073 du 3 août 2016 relatif à la mise à disposition et à la conservation sur support électronique des bulletins de paye et de solde des agents publics

Dernière mise à jour des données de ce texte : 24 décembre 2021

NOR : FCPE1609465D
JORF n°0182 du 6 août 2016

Version en vigueur au 19 mars 2025

Le Premier ministre,
Sur le rapport du ministre des finances et des comptes publics,
Vu l'ordonnance n° 58-1270 du 22 décembre 1958 modifiée portant loi organique relative au statut de la magistrature, notamment son article 42 ;
Vu le code de la défense, notamment son article L. 4123-1 ;
Vu la loi n° 83-634 du 13 juillet 1983 modifiée portant droits et obligations des fonctionnaires, notamment son article 20, ensemble la loi n° 84-16 du 11 janvier 1984 modifiée portant dispositions statutaires relatives à la fonction publique de l'Etat, notamment son article 64 ;
Vu le décret n° 62-765 du 6 juillet 1962 portant règlement sur la comptabilité publique en ce qui concerne la liquidation des traitements des personnels de l'Etat ;
Vu le décret n° 86-83 du 17 janvier 1986 modifié relatif aux dispositions générales applicables aux agents contractuels de l'Etat pris pour l'application de l'article 7 de la loi n° 84-16 du 11 janvier 1984 ;
Vu le décret n° 2010-112 du 2 février 2010 modifié pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;
Vu le décret n° 2010-1690 du 30 décembre 2010 modifié relatif aux procédures financières et comptables spécifiques des forces armées ;
Vu le décret n° 2012-1246 du 7 novembre 2012 modifié relatif à la gestion budgétaire et comptable publique, notamment son article 128 ;
Vu l'avis du Conseil supérieur de la fonction publique de l'Etat en date du 9 février 2016 ;
Le Conseil d'Etat (section de l'administration) entendu,
Décrète :

Article 1

La rémunération après service fait des personnels civils de l'Etat, des magistrats et des militaires, payés sans engagement ni ordonnancement préalable dans les conditions fixées par le décret du 7 novembre 2012 susvisé, donne lieu à la remise aux intéressés d'une pièce justificative dite bulletin de paye.
La rémunération des personnels militaires payée selon la procédure fixée par le décret du 30 décembre 2010 susvisé donne lieu à la remise aux militaires intéressés d'une pièce justificative dite « bulletin de solde ».
Un état annuel indiquant le montant du revenu imposable perçu est également communiqué à chaque agent concerné.

Article 2

Les documents mentionnés à l'article 1er sont mis à disposition des agents concernés sous forme électronique, dans un espace numérique propre, créé et administré par la direction générale des finances publiques et selon des modalités garantissant la sécurité et l'intégrité des données, leur confidentialité et leur accessibilité.

Article 3

Modifié par Décret n°2021-1752 du 21 décembre 2021 - art. 1

Les documents enregistrés dans l'espace numérique sont conservés tout au long de la carrière de l'agent et jusqu'à ce que celui-ci atteigne l'âge de soixante-quinze ans.

Article 4

L'agent reçoit de la direction générale des finances publiques, sous réserve qu'il ait fourni une adresse électronique valide, une notification par voie électronique l'informant de la mise à disposition sur son espace numérique sécurisé du bulletin et de l'état annuel mentionnés à l'article 1er.

Article 5

Dans chaque département ministériel, les articles 1er à 4 entrent en vigueur à une date et selon les modalités fixées par arrêté ministériel, au plus tard au 1er janvier 2020. L'arrêté ministériel précise également la date à partir de laquelle le bulletin de paye sur support papier cesse d'être émis.

Article 6

Par dérogation aux dispositions des articles 2 et 5, il est fait droit aux demandes tendant à bénéficier d'une remise sur support papier des documents mentionnés à l'article 1er, présentées :
1° Par les agents qui sont dans l'incapacité d'accéder sur leur lieu de travail à leur espace numérique sécurisé ;
2° Le temps de ces congés, par les agents bénéficiaires de l'un des congés pris en application des 2°, 3° ou 4° de l'article 34 de la loi du 11 janvier 1984 susvisée, des articles 12, 13, 14 et 16 du décret du 17 janvier 1986 susvisé, de l'article 69 de l'ordonnance du 22 décembre 1958 susvisé, ou du a du 1° de l'article L. 4138-2 du code de la défense.
Chaque arrêté ministériel précise les conditions de dépôt des demandes de copie sur support papier des documents prévus à l'article 1er ainsi que les situations professionnelles dans lesquelles les agents peuvent bénéficier de la dérogation prévue au 1°.
Les copies prévues à l'alinéa précédent sont délivrées par les agents chargés des ressources humaines spécialement habilités par l'autorité administrative, à raison de leurs attributions de gestion financière des personnels relevant de leur ministère, institution ou service, à accéder aux documents cités à l'article 1er.

Article 7

Modifié par Décret n°2021-1752 du 21 décembre 2021 - art. 1

Les établissements publics de l'Etat peuvent mettre à disposition de leurs agents l'espace numérique mentionné à l'article 2 dans les conditions prévues aux articles 2 à 4. Le calendrier et les modalités de cette mise à disposition sont précisés par arrêté conjoint du ministre de tutelle et du ministre chargé du budget, après délibération de l'organe délibérant de l'établissement. Cet arrêté précise les conditions de remise d'une copie du bulletin de paye sur support papier à ces personnels.

Le secrétariat général du Conseil constitutionnel peut mettre à disposition de ses agents l'espace numérique mentionné à l'article 2 dans les conditions prévues aux articles 2 à 4 et suivant un calendrier et des modalités arrêtés par le secrétaire général du Conseil constitutionnel.

Les groupements nationaux d'intérêt public peuvent mettre à disposition de leurs agents l'espace numérique mentionné à l'article 2 dans les conditions prévues aux articles 2 à 4. Le calendrier et les modalités de cette mise à disposition peuvent être précisés par convention approuvée par délibération de l'organe délibérant du groupement.

Les collectivités territoriales, leurs établissements publics et les établissements et services sociaux et médico-sociaux mentionnés à l'article L. 312-1 du code de l'action sociale et des familles peuvent mettre à disposition de leurs agents l'espace numérique mentionné à l'article 2 dans les conditions prévues aux articles 2 à 4. Le calendrier et les modalités de cette mise à disposition peuvent être précisés par convention approuvée par décision de l'organe délibérant de la collectivité, de l'établissement, du service social ou médico-social ou de l'établissement public local.

Les établissements publics de santé mentionnés à l'article L. 6141-1 du code de la santé publique peuvent mettre à disposition de leurs agents l'espace numérique mentionné à l'article 2 dans les conditions prévues aux articles 2 à 4. Le calendrier et les modalités de cette mise à disposition peuvent être précisés par convention approuvée par décision du conseil de surveillance de l'établissement de santé.

Article 8

Le ministre des affaires étrangères et du développement international, la ministre de l'environnement, de l'énergie et de la mer, chargée des relations internationales sur le climat, la ministre de l'éducation nationale, de l'enseignement supérieur et de la recherche, le ministre des finances et des comptes publics, la ministre des affaires sociales et de la santé, le ministre de la défense, le garde des sceaux, ministre de la justice, la ministre du travail, de l'emploi, de la formation professionnelle et du dialogue social, le ministre de l'aménagement du territoire, de la ruralité et des collectivités territoriales, le ministre de l'intérieur, le ministre de l'agriculture, de l'agroalimentaire et de la forêt, porte-parole du Gouvernement, la ministre du logement et de l'habitat durable, le ministre de l'économie, de l'industrie et du numérique, la ministre de la culture et de la communication, la ministre des familles, de l'enfance et des droits des femmes, la ministre de la fonction publique, le ministre de la ville, de la jeunesse et des sports, la ministre des outre-mer et le secrétaire d'Etat chargé du budget sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Fait le 3 août 2016.

Manuel Valls
Par le Premier ministre :

Le ministre des finances et des comptes publics,
Michel Sapin

Le ministre des affaires étrangères et du développement international,
Jean-Marc Ayrault

La ministre de l'environnement, de l'énergie et de la mer, chargée des relations internationales sur le climat,
Ségolène Royal

La ministre de l'éducation nationale, de l'enseignement supérieur et de la recherche,
Najat Vallaud-Belkacem

La ministre des affaires sociales et de la santé,
Marisol Touraine

Le ministre de la défense,
Jean-Yves Le Drian

Le garde des sceaux, ministre de la justice,
Jean-Jacques Urvoas

La ministre du travail, de l'emploi, de la formation professionnelle et du dialogue social,
Myriam El Khomri

Le ministre de l'aménagement du territoire, de la ruralité et des collectivités territoriales,
Jean-Michel Baylet

Le ministre de l'intérieur,
Bernard Cazeneuve

Le ministre de l'agriculture, de l'agroalimentaire et de la forêt, porte-parole du Gouvernement,

Envoyé en préfecture le 26/05/2025
Reçu en préfecture le 26/05/2025
Publié le
ID : 069-256910183-20250523-CS_2025_05_4-DE

Stéphane Le Foll

La ministre du logement et de l'habitat durable,
Emmanuelle Cosse

Le ministre de l'économie, de l'industrie et du numérique,
Emmanuel Macron

La ministre de la culture et de la communication,
Audrey Azoulay

La ministre des familles, de l'enfance et des droits des femmes,
Laurence Rossignol

La ministre de la fonction publique,
Annick Girardin

Le ministre de la ville, de la jeunesse et des sports,
Patrick Kanner

La ministre des outre-mer,
George Pau-Langevin

Le secrétaire d'Etat chargé du budget,
Christian Eckert

Envoyé en préfecture le 26/05/2025
Reçu en préfecture le 26/05/2025
Publié le
ID : 069-256910183-20250523-CS_2025_05_4-DE

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

FINANCES PUBLIQUES

Convention de partenariat entre
Syndicat Intercommunal des Technologies de l'Information pour les Villes (SITIV)
et la Direction générale des Finances publiques
en vue de l'exposition de documents de rémunération
sur le portail ENSAP

Entre :

Syndicat Intercommunal des Technologies de l'Information pour les Villes, représenté par Monsieur Vangheluwe Stéphane, Directeur Général des Services, 50 bd Ambroise Croizat 69200 Vénissieux ci-après dénommé « SITIV », d'une part,

et :

La Direction générale des Finances publiques au sein du ministère de l'Économie, des Finances et de l'Industrie, représentée par Monsieur David KARLE, sous-directeur, responsable du département du programme de modernisation au service des Retraites de l'État, 10 boulevard Gaston Doumergue 44 964 Nantes Cedex 9, ci-après dénommée « la DGFiP », d'autre part,

ci-après collectivement dénommées « les parties ».

il est convenu ce qui suit :

Envoyé en préfecture le 26/05/2025
Reçu en préfecture le 26/05/2025
Publié le
ID : 069-256910183-20250523-CS_2025_05_4-DE

Préambule

La Direction générale des Finances publiques met en œuvre le traitement dénommé ENSAP (Espace numérique sécurisé des agents publics) qui a notamment pour finalité de mettre à la disposition des agents publics un espace d'archivage de documents relatifs à la paye. Ce traitement est autorisé par le décret n°2022-1446 du 21 novembre 2022, pris pour l'application du décret n°2016-1073 du 3 août 2016 relatif à la mise à disposition et à la conservation sur support électronique des bulletins de paye et de solde des agents publics, modifié par décret n°2021-1752 du 21 décembre 2021 relatif aux modalités d'utilisation par certaines personnes morales de droit public de l'espace numérique sécurisé des agents publics et modifiant la durée de conservation des données au sein de ce traitement.

Ce traitement a été soumis à avis préalable de la CNIL rendu dans sa délibération n° 2022-109 du 10 novembre 2022.

L'Espace Numérique Sécurisé de l'Agent Public (ENSAP), offre de service internet sécurisée développée et administrée par la DGFiP, améliore et simplifie l'accès des agents à leurs documents de rémunération (bulletins de paye ou de salaire, décomptes de rappel, attestations fiscales), en les mettant à leur disposition sous forme dématérialisée dans un espace personnel performant et ergonomique, accessible par internet 7 jours sur 7.

L'agent dispose de deux modalités distinctes d'accès à l'espace numérique sécurisé : par un dispositif d'authentification (DAC/LDAP) spécifique par un couple login (NIR) - mot de passe, ainsi que par le service FranceConnect qui est un mécanisme de fourniture d'identité et d'authentification numérique pour les usagers. FranceConnect permet également le suivi par l'usager des échanges de données le concernant et garantit la confidentialité des informations.

Article 1. Objet de la convention

Le présent document a pour objet de définir les conditions et modalités de collaboration entre la DGFiP et SITIV en vue d'exposer dans l'ENSAP les documents de paye des agents rémunérés par ce dernier.

La présente convention vaut convention de mise à disposition de l'ENSAP auprès des agents de SITIV au sens de l'article 7 du décret n° 2016-1073 du 3 août 2016 modifié relatif à la mise à disposition et à la conservation sur support électronique des bulletins de paye et de solde des agents publics.

Article 2. Suivi des questions de sécurité

- L'AQSSI (Autorité Qualifiée pour la Sécurité des Systèmes d'Information) de Ia DGFIP est le Directeur général des Finances publiques. Le RSSI (Responsable de la Sécurité des Systèmes d'Information) représente l'AQSSI de la DGFiP. En particulier, la sécurité de l'ENSAP fait partie de son périmètre de responsabilité. Ces fonctions sont exercées par le responsable de la division DMOCSS et par son adjoint, par délégation.

- Pour SITIV, l'AQSSI est le Directeur Général des Services de l'intéressé . Le RSSI (Responsable de la Sécurité des Systèmes d'Information) représente l'AQSSI sur les aspects opérationnels et est l'interlocuteur unique de la DGFiP pour ce qui concerne les dispositions de sécurité relevant de la présente convention. Le périmètre de ses responsabilités comprend :

le contrôle du respect des règles d'emploi et de sécurité de l'ENSAP définies par la DGFIP,

le transfert des données vers l'ENSAP.

Article 3. Rôle et engagements de la DGFIP

La DGFiP agit en tant que fournisseur de service, et, à ce titre, doit assurer la sécurité et la confidentialité des informations personnelles lorsqu'elles transitent et sont stockées dans son système d'informations et ce dès leur prise en charge.

La DGFiP met en œuvre et opère les échanges des données et des flux conformément aux dispositions réglementaires et légales en vigueur.

La DGFiP est responsable des données reçues, traitées, stockées, diffusées par l'ENSAP, y compris les données techniques afférentes. A ce titre, elle garantit la bonne utilisation de l'ENSAP par toutes les parties prenantes au système et détermine les conditions d'utilisation, les règles d'emploi et de sécurité du système et veille à leur respect.

La DGFiP réalise les développements informatiques nécessaires au fonctionnement des services. Elle assure l'hébergement et l'exploitation des applicatifs et de toute l'infrastructure nécessaire au fonctionnement des back et front offices.

La DGFiP s'engage sur une simple mise à disposition des documents transmis par le fournisseur de données, à l'exclusion de toute autre utilisation des données et documents transmis par celui-ci. À réception des flux, la DGFIP assure la restitution d'un accusé de traitement par ATLAS et d'un fichier retour fonctionnel de collecte des données par l'ENSAP.

L'offre générale de mise à disposition des documents est adossée à une offre d'archivage des documents PDF dans le silo ATLAS, jusqu'aux 75 ans de l'usager ou jusqu'à deux ans après son décès.

Il est rappelé que, conformément à l'article 1 du décret n°2022-1446 du 21 novembre 2022 précité, la mise en œuvre du traitement ENSAP par la DGFiP est nécessaire au respect d'une obligation légale.

La mise à disposition des bulletins de paie des agents ne nécessite aucune option particulière de ces derniers (*référence de la décision du conseil de surveillance ou de l'organe délibérant de la collectivité ou de l'établissement public* de *SITIV* du *date* portant application du décret n° 2016-1073 du 3 août 2016 modifié relatif à la mise en place et à la conservation sur support électronique des bulletins de paye et de solde des agents publics).

La DGFiP présente à l'usager tous les éléments d'informations nécessaires pour l'utilisation du Portail. Le Portail est accessible aux agents de SITIV à un niveau de disponibilité dit « fort » au sens de la DGFIP (cf. annexe 1). La durée de conservation des données d'identification et des logs ENSAP est de 12 mois à compter de leur enregistrement.

La DGFiP ne peut intervenir sur les données de SITIV sans son autorisation explicite. Elle s'engage à fournir à SITIV toutes les informations utiles et nécessaires en cas d'événement de sécurité de nature à affecter le système d'information dont elle est responsable.

Sur la sollicitation de SITIV, la DGFiP s'engage à coopérer avec lui/elle, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à permettre l'exercice, par les personnes concernées, de leurs droits d'accès et de rectification prévus par la réglementation.

Article 4. Rôle et engagements du SITIV

Dans le cadre du Portail ENSAP, SITIV est fournisseur de données. Il s'engage à transmettre les données et documents personnels nécessaires à l'application de la présente convention et à ne pas communiquer de données non utiles à celle-ci.

Il incombe à SITIV de supprimer de ses envois vers la DGFiP les informations qu'il jugerait très sensibles ou incompatibles avec le niveau de protection mis en œuvre par ce dernier. Notamment, les informations relevant d'une diffusion restreinte ne doivent pas être transmises à la DGFIP.

Il incombera à SITIV d'informer ses personnels de toute modification qui serait introduite sur les documents ou données transmises.

Le SITIV s'engage à transmettre les métadonnées et bulletins de paie au format PDF/A après chiffrement, conformément au format d'échange technique décrit dans la documentation fournie lors de l'ouverture du projet (DGFiP : SSI et SRE ; le SITIV).

[Les flux seront transmis via le réseau interministériel de l'Etat (RIE) et devront être chiffrés.]

La DGFiP refusera la réception des flux non conformes aux spécifications techniques.

Le SITIV s'engage à fournir à la DGFiP toute information utile et nécessaire en cas d'événement de sécurité de nature à affecter le système d'information dont elle est responsable.

Article 5. Obligations relevant du règlement européen n° 2016/679 du 27 avril 2016, de la loi n° 78-17 du 6 janvier 1978 modifiée par la loi 2018-493 du 20 juin 2018 et du décret n°2010-112 du 2 février 2010

La DGFiP, en tant que co-traitant, et le SITIV, en tant que fournisseur de données, s'engagent à respecter les obligations inhérentes aux échanges induits par l'ENSAP, notamment celles, détaillées ci-dessous, relevant de la loi n° 78-17 du 6 janvier 1978 modifiée par la loi 2018-493 du 20 juin 2018 relative à la protection des données personnelles, celles du règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et celles relevant de l'ordonnance n°2005-1516 du 8 décembre 2005 et du décret n°2010-112 du 2 février 2010 relative au Référentiel Général de Sécurité.

La confidentialité et la disponibilité des données à caractère personnel durant toute l'exécution de la présente convention et après son expiration.

La prise de toutes mesures nécessaires telles que définies aux articles 6 et 7 de la présente convention pour préserver la sécurité et la confidentialité des données et empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

- Effectuer les formalités auxquelles la DGFIP et le SITIV sont astreint(e)s en tant que responsables de traitement de leur système d'information respectif. Les informations sur la réalisation de celles-ci doivent être communiquées à la partie qui en fait la demande.

- Répondre aux usagers concernant leurs demandes de droit d'accès et de rectification. Ces droits s'exercent pour les données concernant la paye auprès de le SITIV et pour les données d'authentification et de connexion au portail ENSAP auprès de la DGFIP.

Article 6. Confidentialité des données et secret professionnel

Les parties sont tenues, ainsi que l'ensemble de leur personnel, au secret professionnel, à l'obligation de discrétion et à l'obligation de confidentialité durant toute l'exécution de la présente convention et après son expiration.

Les parties conviennent que les données transmises à la DGFiP ne doivent en aucun cas être divulguées ou retransmises à des personnes physiques ou morales non autorisées.

Les parties s'interdisent toute communication d'informations écrite ou verbale sur ces sujets ou toute remise de documents à des tiers sans l'accord préalable et écrit de l'autre partie.

Les parties s'engagent à respecter de façon absolue lesdites règles et obligations, et à les faire respecter par les utilisateurs qu'ils auront autorisés à accéder aux services.

Si, pour l'exécution de la présente convention, les parties ont recours à des prestataires de services traitant des données à caractère personnel pour le compte du responsable du traitement, ceux-ci doivent être considérés comme des sous-traitants au sens de la loi 78-17 du 6 janvier 1978 modifiée et présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité. Cette exigence ne décharge pas le responsable de traitement de son obligation de veiller au respect de ces mesures.

Le contrat liant le sous-traitant au responsable du traitement doit comporter toutes les indications permettant le respect des dispositions de l'article 28 du règlement européen sur la protection des données n° 2016/679.

<u>Contrôle sur les personnels en charge d'intervenir et de maintenir les applications</u>

Les parties s'engagent à faire souscrire à ces prestataires de services, en plus des engagements contenus dans le présent article, les engagements suivants :

- ils ne doivent pas utiliser les documents et supports d'information confiés par l'une des parties à des fins autres que celles spécifiées à la convention,
- ils ne doivent conserver aucune copie des documents et supports d'information confiés par l'une des parties après l'exécution des prestations,
- ils ne doivent pas communiquer ces documents et informations à d'autres personnes que celles qui ont qualité pour en connaître,
- ils doivent prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers en cours d'exécution de la présente convention,
- ils doivent prendre toutes mesures, notamment de sécurité matérielle, pour assurer la conservation des documents et informations traités tout au long de la convention,

- ils doivent reconstituer les documents et les fichiers qui leur sont confiés et qui viendraient à être perdus ou inutilisables par leurs fautes.

Dans le cas où les prestataires de services sous-traiteraient l'exécution des prestations à un tiers, ce dernier serait soumis aux mêmes obligations.

Article 7. Sécurité

Les parties s'engagent à prendre toutes les mesures utiles pour assurer, lors de l'exécution de la convention, la protection des informations ou supports protégés qui peuvent être détenus ou échangés par les parties.

La mise en œuvre de certificats avec authentification mutuelle est obligatoire pour tout échange, de même que l'implémentation rigoureuse des règles d'appels telles que définies dans l'annexe 4 en conformité avec le RGS. Les deux parties s'engagent à se communiquer toute information utile et nécessaire en cas d'événement de sécurité.

La DGFiP est responsable de l'homologation de sécurité du Portail ENSAP et de son maintien en condition de sécurité.

Sur demande, chacune des parties communiquera la décision d'homologation de son système d'information visé par la présente convention de partenariat.

Le site ensap.gouv.fr est un site du Ministère en charge de l'Économie, des Finances et de l'Industrie, dont les modalités d'utilisation sont encadrées par le décret n°2022-1446 du 21 novembre 2022 précité.

Article 8 : Protection des données à caractère personnel et notification des violations de données personnelles

SITIV et la DGFIP, sont co-responsables du traitement des données de l'ENSAP pour les agents rémunérés par SITIV.

SITIV s'engage à informer ses agents de la mise en œuvre du traitement ENSAP, ainsi que des conditions dans lesquelles ils peuvent demander l'accès, la rectification de leurs données personnelles. SITIV informe ses agents des coordonnées de son DPO.

8-1. Gestion des incidents de sécurité, notamment les violations de données à caractère personnel

Les Parties gèrent les incidents de sécurité, y compris les violations de données à caractère personnel, conformément à leurs procédures internes et à la législation applicable.

Les Parties se prêtent en particulier mutuellement une assistance rapide et efficace, le cas échéant, pour faciliter l'identification et la gestion de tous les incidents de sécurité, notamment les violations de données à caractère personnel, liées à au traitement conjoint.

Les Parties se notifient mutuellement:

a) tout risque potentiel ou réel pour la disponibilité, la confidentialité, et / ou l'intégrité des données à caractère personnel traitées conjointement ;

b) tout incident de sécurité lié au traitement conjoint ;

c) toute violation de données à caractère personnel (c'est-à-dire toute violation de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la

divulgation non autorisée de données à caractère personnel ou l'accès non autorisé aux données traitées conjointement) ;

d) toute faille dans les garanties techniques ou organisationnelles de l'opération de traitement conjointe.

La notification de violation des données à caractère personnel aux autres responsables conjoints contient au-moins :

- la description de la nature de la violation des 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 ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- l'évaluation du risque pour les droits et libertés des personnes physiques ;
- la description des mesures prises pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Chaque Partie est responsable de tous les incidents de sécurité, y compris les violations de données à caractère personnel, qui se produisent en conséquence d'une violation des obligations de cette partie en vertu de cet accord et du Règlement (UE) 2016/679.

Les Parties documentent les incidents de sécurité (y compris les violations de données à caractère personnel) et se les notifient mutuellement dans les meilleurs délais et au plus tard 72 heures après avoir pris connaissance d'un incident de sécurité (y compris une violation de données à caractère personnel).

La Partie, responsable d'une violation de données à caractère personnel, documente cette violation de données à caractère personnel et la notifie à la Commission nationale de l'informatique et des libertés. Cette notification doit être effectuée dans les meilleurs délais et, si possible, 72 heures au plus tard après avoir pris connaissance de la violation de données à caractère personnel, à moins que la violation de données ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. La Partie responsable doit informer les autres parties de cette notification.

La Partie, responsable de la violation de données à caractère personnel, communique cette violation de données à caractère personnel aux personnes concernées si la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. La Partie responsable doit informer les autres Parties de cette communication.

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 du responsable conjoint concerné 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 pour remédier à la violation y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

8-2. Coordonnées des RSSI et DPD

RSSI SITIV :

Hibert Sylvain
RSSI

Ou par mail : shibert@sitiv.fr

RSSI DGFiP : Monsieur le Directeur général des Finances publiques
Monsieur le responsable de la division DMOCSS
bureau.si3-dmocss@dgfip.finances.gouv.fr

DPD SITIV :

Hibert Sylvain
DPD

Ou par mail : shibert@sitiv.fr

DPD DGFiP :

Monsieur le délégué à la protection des données du ministère économique et financier
Délégation aux Systèmes d'Information
139, rue de Bercy Télédoc 322. 75572 PARIS CEDEX 12
le-delegue-a-la-protection-des-donnees-personnelles@finances.gouv.fr

Article 9 : Circuit d'assistance

Le circuit d'assistance aux agents est décrit dans le Guide du gestionnaire de la paie remis à le SITIV. Il emporte toutes les conséquences liées à des défaillances portées par les flux de documents de paie : inscription à l'ENSAP, accès au service d'exposition des documents de paie.

Pour tout autre question des internautes sur le portail, l'internaute dispose d'un assistant virtuel et de FAQ.

Article 10 : Rétrocession des documents transmis par l'employeur

Le silo de stockage ATLAS, de la DGFiP, prévoit la possibilité, pour l'émetteur de documents PDF conservés dans ce silo, de rétrocéder ces documents, sur la base d'une demande expressément formulée à l'adresse électronique suivante : bureau.bsi2-atlas@dgfip.finances.gouv.fr. Cette rétrocession entraînera : la restitution à l'émetteur originel de l'ensemble des documents demandés, ainsi que la purge de ces mêmes documents de la plateforme ATLAS. ATLAS informera l'ENSAP des documents dont il conviendra de purger les métadonnées correspondantes.

Article 11 : Évolutions

La DGFIP s'engage à prévenir le SITIV de tout projet d'évolution des flux et des spécifications associées avec un délai de prévenance trois mois. Le nouveau format de flux sera mis en production par l'ENSAP en tenant compte du délai de réalisation des évolutions par le SITIV pour son propre flux de collecte.

Article 12. Durée, modification et résiliation de la convention

La présente convention prend effet à compter de sa date de signature, pour une durée indéterminée.

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

Elle reste valable tant que l'une ou l'autre des parties ne l'aura pas dénoncée. Si l'une des parties souhaite résilier la présente convention, elle en informe l'autre partie, par écrit, en indiquant les motifs de sa décision. Un préavis de 12 mois est alors nécessaire avant que la résiliation ne soit pleinement effective. Durant cette période, les deux parties s'engagent à assurer le service dans les conditions de cette convention.

Les documents précédemment archivés jusqu'à la date de résiliation resteront archivés durant toute la carrière des personnels de le SITIV et jusqu'à leurs 75 ans ou jusqu'à deux ans après leur décès.

Les stipulations des articles 5 à 9 de la présente convention restent en vigueur après sa cessation pour quelque cause que ce soit.

Fait en deux exemplaires originaux,

A Vénissieux , le 18 mars 2025 Pour le SITIV Monsieur Stéphane Vangheluwe DGS	A Nantes, le Pour la Direction générale des Finances publiques Monsieur David KARLE Sous-directeur, responsable du département du programme de modernisation Service des retraites de l'État

Envoyé en préfecture le 26/05/2025
Reçu en préfecture le 26/05/2025
Publié le
ID : 069-256910183-20250523-CS_2025_05_4-DE

Annexe 1

Qualité de service Portail ENSAP :
Le niveau de disponibilité est dit "fort" au sens DGFIP. Ainsi, les exigences pour ce niveau de disponibilité sont les suivantes :

- Portail : ouvert toute l'année.
- Périodes sensibles identifiées : premiers jours de chaque mois, ainsi que lors de la période de délivrance de l'attestation fiscale
- Plages d'ouverture du service pour les usagers : 22h/24h 7/7j. Maintenance réservée plage 01h00 et 03h00
- Accessible via internet
- Pas de besoin d'astreintes les soirs et les week-end.
- Garantie du temps de rétablissement en cas d'incident estimée à 8 heures ouvrées.
- Taux de disponibilité des plages de couverture : 97 %.
- Navigation adaptée à tout support (PC, smartphone, tablettes), compatibilité avec de nombreux navigateurs internet.

Annexe 2

La DGFiP opère un cloisonnement strict des différents réseaux qui composent son SI, conformément aux principes de base recommandés par l'ANSSI. Ce cloisonnement réseau vise à protéger le système d'information et les données qui y sont stockées et traitées, en découpant notamment différents sous-ensembles selon leur sensibilité, tout en y apportant des infrastructures de détection, de contrôle et de traçabilité dédiées.

L'administration de tous les équipements (réseau et applicatifs) est notamment faite au travers d'un réseau dit « d'administration » dédié, totalement décorrélé des réseaux bureautiques.

Les accès aux applicatifs ENSAP seront authentifiés et tracés au travers de dispositifs d'accès et de contrôle, basés sur des annuaires centralisés. Le niveau de privilège associé aux accès est aussi défini au niveau de ces annuaires pour ce qui est de la population agents DGFiP. Les accès usager sont aussi authentifiés et tracés.

Annexe 3

Les mesures de sécurités relatives à l'accès physique au bâtiment et protection des machines

- Sécurité générale des établissements des services informatiques de la DGFiP.

- Sécurité physique des matériels et de l'accès aux informations :

✓ Protection incendie : Les établissements sont dotés de moyens de détection d'incendie avec alarme et/ou déclenchement de dispositifs automatiques d'extinction.

✓ Protection contre les agressions et les vols : les établissements font l'objet d'un renforcement des protections périmétriques (clôtures…) et rapprochées (vitrages anti-effraction…) et sont directement reliés avec le commissariat de police le plus proche.

Pendant les heures de travail, l'accès à l'établissement est contrôlé (badges et registre pour les visiteurs).
La nuit, l'établissement est :
- soit surveillé par un veilleur de nuit ;
- soit fermé et gardé par un système de télésurveillance.
Les jours non ouvrés, l'établissement est :
- soit fermé et gardé par un gardien concierge logé sur place
- soit fermé et gardé par un système de télésurveillance.
L'accès à la salle ordinateur est limité aux seules personnes autorisées par système de badge et les bandothèques sont toujours fermées à clé, sous la responsabilité du chef bandothécaire ou du chef d'exploitation.

- Machines localisées dans un Service de Production Sécurisé (SPS)

L'application est installée dans une salle blanche du site d'hébergement. Ce site présente les caractéristiques suivantes en matière de sécurité :

✓ Détection incendie ;
✓ Extinction incendie ;
✓ Gestion Technique du Bâtiment (GTB) ;
✓ Contrôle d'accès ;
✓ Vidéosurveillance ;
✓ Contrôle anti-intrusion.

La sécurisation du site a été prise en compte dès sa conception tant dans sa dimension passive qu'active :

La sécurisation passive concerne les dispositions constructives prises sur l'architecture et la structure du site et permet d'assurer :

✓ la protection des locaux contre des agressions venant de l'extérieur,
✓ l'impossibilité ou le ralentissement d'une intrusion abusive dans les différentes zones protégées intérieures,
✓ la protection des ouvertures dans les parois nécessaires au fonctionnement des équipements techniques, comme les prises d'air et les rejets, ainsi que les équipements nécessairement disposés à l'extérieur (dry-cooler, par exemple).

La sécurisation active concerne les dispositifs de contrôle, de détection et de surveillance mis en place sur le site. Elle permet de suivre en temps réel l'évolution d'une personne à l'intérieur ou à l'extérieur du bâtiment. Elle intègre :

✓ le contrôle d'accès extérieur et intérieur,
✓ la surveillance / détection par caméras vidéo,
✓ le contrôle d'intrusion.

Pour répondre aux objectifs de sécurité, le site a été organisé en différentes zones présentant des caractéristiques de sécurité adaptées aux enjeux. Le but est d'empêcher l'accès non autorisé au centre informatique et limiter l'impact d'une malveillance ou d'un incendie sur les systèmes d'information.

Les infrastructures de traitement de l'information cruciales ou sensibles sont situées dans une zone limitée par un périmètre de sécurité défini, avec des barrières de sécurité et des mesures de contrôle appropriées à l'entrée. Elles sont protégées physiquement contre les menaces définies. La protection physique est obtenue en créant plusieurs barrières physiques autour du centre informatique.

Trois zones de sécurité seront établies, chacune d'entre elles augmentant la protection totale fournie.

- ✓ Zone Campus : cette zone est définie par la clôture périphérique du terrain. L'accès au campus s'effectue exclusivement sous contrôle du gardien au travers d'un accès véhicule et un accès piétons ;
- ✓ Zone d'accueil : cette zone est définie par l'atrium limité par son enceinte vitrée. Elle constitue une zone de transition entre la zone Campus et la zone Bâtiments. Elle est placée sous contrôle permanent d'un gardien ;
- ✓ Zone bâtiment : cette zone est définie par l'enceinte des trois bâtiments. La zone est limitée par les murs extérieurs, la toiture constituée d'un bac acier supportant une isolation par laine de roche et une étanchéité par revêtement goudronné et enfin au sol la dalle béton. Les ouvrants de la façade sont maintenus fermés par des fixations indémontables. Les baies et ouvrants sont condamnés par l'intérieur, par un bardage acier fixé sur la structure béton. Les issues de secours font l'objet d'une protection mécanique et d'un verrouillage par un dispositif conforme à la réglementation.

L'accès aux bâtiments s'effectue après enregistrement auprès du gardien à la zone d'accueil. L'accès aux bâtiments 1 et 2 renfermant les locaux informatiques fait l'objet d'un contrôle par badge. L'accès est équipé d'un sas. L'accès aux zones informatiques est contrôlé par badge.

Quatre populations accèdent au site :

- ✓ les personnels informatiques,
- ✓ les personnels techniques,
- ✓ les personnels de gardiennage,
- ✓ les visiteurs.

Pour assurer la sécurité du centre ainsi que leur propre sécurité, les personnels et visiteurs doivent se soumettre à tous les contrôles et procédures requises par le plan de sécurité. Le port du badge visible est obligatoire et les personnels sont encouragés à interroger tout visiteur sans escorte ou toute personne ne portant pas d'identification visible.

En matière de sécurité intrusion, aucun signe extérieur ne marque la présence du centre informatique ou ne révèle l'identité de l'occupant. La signalétique est anonyme et ne permet pas de déduire l'activité du centre. L'éclairage est diffus, les dispositifs de surveillance extérieure (détecteurs, caméras…) discrets. Aucun véhicule ne doit stationner en dehors des zones parking. L'arrêt sur les zones livraison est limité au temps nécessaire au chargement ou au déchargement.

Les zones de services (photocopieurs, télécopieurs) et les commodités sont en dehors des zones informatiques ou techniques. A chaque périmètre de sécurité est mise en œuvre une surveillance électronique :

- ✓ Zone Campus : La clôture extérieure est équipée d'une détection de chocs sur clôture et de contacts d'ouverture sur les portails et portillons. Les accès extérieurs et les zones extérieures font l'objet d'une vidéosurveillance.
- ✓ Zone bâtiment : Les baies, ouvrants et issues de secours situés au rez-de-chaussée sont surveillées par une détection choc et ouverture. Les toitures sont surveillées par des barrières infra-rouge couplées au système de vidéosurveillance couvrant la zone. Les salles informatiques sont mises sous contrôle du système de vidéosurveillance. Les locaux inoccupés sont fermés à clef et mis sous contrôle du système de vidéosurveillance. Les circulations et le hall d'accueil font l'objet d'une vidéosurveillance. Les accès contrôlés par badge sont surveillés par contact de choc et ouverture (effraction et porte restée ouverte trop longtemps).

En matière de sécurité incendie, les moyens mis en œuvre sont les suivants :

- ✓ Moyens préventifs : Les zones informatiques sont isolées par une enceinte séparative coupe-feu 2 heures étanche aux fumées et aux fluides. Les salles informatiques sont maintenues en surpression pour éviter une contamination par des fumées venant de l'extérieur. Les armoires techniques climatisation et électricité sont placées dans les couloirs techniques à l'extérieur des zones informatiques. Les matières dangereuses ou inflammables sont stockées en sûreté, à distance des zones informatiques. Les fournitures telles que papier ou supports magnétiques sont stockées en dehors des zones informatiques.
- ✓ Moyens curatifs : Le processus comporte 3 étapes :
  - ✓ Détection automatique rapide et fiable favorisant la réactivité des intervenants ;
  - ✓ Déconnexion de la machine en défaut ou utilisation d'extincteurs portables CO2 ou H2O ;
  - ✓ Recours à une extinction automatique.

Annexe 4

L'ENSAP s'inscrit dans la politique de sécurité de la DGFiP dont l'AQSSI est le garant.
L'application bénéficie à ce titre comme l'ensemble des projets de la DGFiP :

- d'une démarche formelle d'amélioration continue de la sécurité
- d'une sécurisation des données traitées
- d'une détection et gestion des incidents de sécurité
- d'une promotion des mesures de sécurité auprès des utilisateurs
- d'une identification et gestion des risques
- d'un plan de reprise d'activité (PCA) testé régulièrement
- d'un maintien en condition opérationnelle
- d'une homologation par la DGFiP de l'application ENSAP en conformité avec les normes imposées par le RGS. (calendrier et modalités à définir par la DGFIP)

Le SITIV participe à la sécurité du projet en :

- étant destinataire de la politique de sécurité retenue
- respectant les règles d'emploi et de sécurité afférentes au SI ENSAP émanant de la DGFIP,
- dé-sensibilisant les données véhiculées dans les flux, si nécessaire (ex. : suppression de l'adresse postale des usagers),
- chiffrant les échanges et les données
- détectant et gérant les incidents de sécurité sur son système d'information dont il a la maîtrise d'œuvre
- faisant la promotion des mesures de sécurité auprès des utilisateurs
- respectant le format d'échange des données sous peine de rejet de l'intégralité du flux.

Envoyé en préfecture le 26/05/2025
Reçu en préfecture le 26/05/2025
Publié le
ID : 069-256910183-20250523-CS_2025_05_4-DE

ACCORD CADRE PRESTATION DE TELETRANSMISSION SITIV /ENSAP

1 Préambule

La Direction Générale des Finances Publiques met en œuvre le traitement ENSAP qui a pour finalité de mettre à la disposition des agents publics de la Structure un espace d'archivage de documents relatifs à la paie. En tant qu'éditeur de logiciel de paie, SITIV propose aux Structures clientes un service de télétransmission de leurs données et documents vers le portail de l'Espace Numérique Sécurisé de l'Agent Public (ENSAP).

2 Objet

La présente convention a pour objet d'encadrer la mise à disposition d'une clé de chiffrement et l'exécution de la prestation de télétransmission des données vers l'Espace Numérique Sécurisé de l'Agent Public exécutée par SITIV pour le compte des Structures mandantes.

3 Définitions

Structure : Ce terme désigne le cocontractant de SITIV pour la prestation de télétransmission des données et documents vers le portail de l'ENSAP.

DGFiP : Direction Générale des Finances Publiques.

ENSAP : Espace Numérique Sécurisé de l'Agent Public édité et géré par la Direction Générale des Finances Publiques.

Télétransmission : Opération de transmission de documents et données sous format électronique exécutée par SITIV, dans les conditions définies par le corpus contractuel, pour le compte d'une Structure.

4 Documents contractuels

Les pièces qui régissent la Convention sont par ordre de priorité :

- Le présent accord-cadre de Télétransmission SITIV /Ensap et la Convention de Partenariat entre la Structure et la Direction Générale des Finances Publiques en vue de l'exposition de documents de rémunération sur le Portail ENSAP
- Les dispositions contractuelles entre SITIV et la Structure : *(dénomination exacte des dispositions en question à indiquer)*

- Le Mandat de Télétransmission ENSAP en Annexe de la présente Convention.

En cas de contradiction, notamment au sein d'un même document, la volonté des Parties sera recherchée.

5 Prérequis

La signature de cet Accord-Cadre est un préalable à la conclusion de la Convention de chiffrement entre le RSSI (Responsable de la Sécurité des Systèmes d'Informations) de SITIV et le RSSI de la DGFiP. Celle-ci est transmise par cette dernière à la demande de SITIV auprès du RSSI de la DGFiP.

Coordonnées des RSSI :

RSSI de SITIV :

Sylvain Hibert, RSSI

Ou mail : shibert@sitiv.fr

RSSI DGFiP : Madame la Directrice générale des Finances publiques
Monsieur le responsable de la division DMOCSS
bureau.si3-dmocss@dgfip.finances.gouv.fr

À la suite de cette saisine, la DGFiP se chargera d'initier la rédaction de la convention d'échange des clés de chiffrement.
Tous les échanges de clés applicatives doivent obligatoirement transiter par les responsables sécurité des systèmes d'informations, afin qu'ils puissent chacun sursigner les clés. Pour être valide, une clé applicative doit posséder les deux signatures des responsables sécurité.

La mise en œuvre d'une opération de télétransmission pour le compte d'une Structure est conditionnée par la validation des tests de chiffrement et par la signature de ladite convention de chiffrement.

L'opération de télétransmission est également conditionnée par la validation des tests de transmissions des flux.

6 Obligations des Parties

6.1 Obligation de l'ENSAP :

En tant qu'éditeur et gestionnaire de l'Espace Numérique Sécurisé des Agents de la Direction Générale des Finances Publiques :

- S'engage à créer et à mettre à la disposition de SITIV une clé de chiffrement spécifique et unique, avec un niveau de sécurité conforme à l'état de l'art, au moyen de laquelle les prestations de télétransmission en faveur des mandants seront mises en œuvre.

- Réceptionner les données transmises par SITIV dans le cadre de l'exécution de sa prestation de télétransmission, lorsque ces transferts sont conformes aux prérequis techniques tels que définis à l'article 5. Il est entendu que la réalisation de sa prestation d'exposition des documents de rémunération sur le portail ENSAP est régie par la Convention la reliant à la Structure.

- Informer SITIV dans les plus brefs délais de toute non-conformité dans l'exécution de sa prestation de télétransmission, notamment en ce qui concerne le respect des prérequis techniques.

- Informer SITIV, dans les meilleurs délais, de toute problématique technique ayant un impact, direct ou indirect, sur la réalisation de sa prestation de télétransmission par SITIV. La DGFiP s'engage notamment à informer SITIV de tout projet d'évolution des flux et des spécifications associées avec un délai de prévenance de six (6) mois. Le nouveau format de flux sera mis en production par l'ENSAP en tenant compte du délai de réalisation des évolutions par SITIV pour l'ensemble des flux de collecte des Structures pour lesquelles il est mandaté pour réaliser la prestation de télétransmission.

La DGFiP est responsable des données reçues par SITIV, traitées et stockées, diffusées par l'ENSAP, y compris les données techniques y afférentes. Les modalités de traitement des données dans le cadre de l'exécution de la prestation de télétransmission sont précisées en Annexe II.

6.2 Obligation de SITIV:

En tant que tiers-émetteur des données, SITIV bénéficie d'une clé de chiffrement transmise par la Direction Générale des Finances Publiques, avec laquelle SITIV transmettra les flux de données dans les conditions définies à l'Annexe I, pour l'ensemble des Structures mandantes. À ce titre, SITIV bénéficie d'un droit d'utilisation de cette clé de chiffrement pendant toute la durée du présent Accord-Cadre.

SITIV s'engage à utiliser cette clé de chiffrement seulement pour la réalisation des prestations de télétransmission, sur le fondement du mandat dont le modèle est Annexé (annexe 1) avec la Structure, Responsable de Traitement sur les données objets de la prestation.

SITIV s'engage à mettre en œuvre les mesures techniques et organisationnelles adéquates afin de s'assurer de la confidentialité de cette clé de chiffrement et, notamment, pour éviter toute utilisation, divulgation ou modification non autorisée.

SITIV s'engage à transmettre l'ensemble de ces données conformément aux prérequis techniques précisés par la DGFIP à l'article 5. En tant que fournisseur de données, SITIV s'engage à transmettre les

métadonnées et bulletins de paie objets de la prestation au format PDF/A après chiffrement, par sa clé unique.

SITIV s'engage à faire signer l' « Annexe I – Mandat Structure » à l'ensemble des Structures souhaitant utiliser le service de télétransmission tel que défini dans le présent Accord-Cadre.

La DGFIP s'autorise à refuser la réception des flux non conformes aux spécifications techniques. Dans cette hypothèse, la DGFIP s'engage à en informer SITIV, par écrit, dans les meilleurs délais.

6.3 Obligations communes

Chaque Partie s'engage à conserver secrètes et confidentielles, autrement que pour les seuls besoins d'exécution de la Convention, toutes Informations, procédures, données, méthodes, prototypes, créations, licences, droits de propriété intellectuelle, savoir-faire et documents de quelque nature que ce soit dont les Parties ont pris connaissance pour la mise en œuvre ou lors de l'exécution de la Convention. Les Parties s'engagent à faire respecter les dispositions du présent article à leurs employés, collaborateurs, sous-traitants et tout tiers susceptible d'intervenir dans le cadre de la Convention.

Dans le cas où la communication des Informations Confidentielles est imposée par l'application d'une disposition légale ou réglementaire ou dans le cadre d'une procédure judiciaire, administrative ou arbitrale, cette communication doit être limitée au strict nécessaire. La Partie réceptrice s'engage, sauf disposition expresse contraire, à informer immédiatement et préalablement à toute communication la Partie émettrice afin de permettre à cette dernière de prendre les mesures appropriées à l'effet de préserver leur caractère confidentiel.

Les obligations de confidentialité stipulées au présent article resteront en vigueur après l'arrivée à échéance du présent Accord ou de la date de résiliation de dernier.

Les Parties s'engagent à ne pas perturber, entraver ou fausser, directement ou indirectement, le fonctionnement du service et de l'infrastructure de l'autre, par quelque moyen que ce soit.

Les Parties s'engagent à informer l'autre de toute erreur, irrégularité, faute ou acte illicite ou contraire disposition de la Convention constatée dans le cadre de l'exécution des prestations objets de la Convention.

7 Responsabilité

La responsabilité de SITIV ne peut être engagée que pour les préjudices nés directement de l'exécution de l'opération de transmission pour le compte de la Structure.

La responsabilité de la DGFiP ne peut être engagée que pour les préjudices nés à compter de la réception conforme des données et documents, dans le périmètre des obligations qui sont les siennes, en application de la présente Convention et de celle la reliant à la Structure.

La responsabilité de l'une ou l'autre Partie ne pourra être engagée en cas d'inexécution, de mauvaise exécution ou de retard dans l'exécution de tout ou partie des Prestations objets de l'accord-cadre qui serait due au non-respect par l'autre de ses obligations contractuelles ou à l'indisponibilité des moyens que cette dernière doit fournir.

8 Sous-Traitance

Chaque partie peut librement recourir à la sous-traitance dans le respect des dispositions législatives et réglementaires en vigueur, sous réserve d'en informer préalablement son cocontractant. Elle s'assure que ses sous-traitants présentent les garanties et qualifications professionnelles nécessaires à la réalisation de la prestation sous-traitée dans les conditions définies par la présente Convention. La Partie en cause garantit son cocontractant de l'exécution conforme à la présente Convention des prestations sous-traitées.

9 Propriété Intellectuelle

La Convention n'aura pas pour effet de modifier ou d'altérer les éléments et/ou droits de propriété intellectuelle et industrielle au sens du Code de la Propriété Intellectuelle détenus par chacune des Parties. La mise à disposition par l'une des Parties de tout élément quel qu'il soit dans le cadre de la Convention ne saurait être considérée comme un transfert ou une cession au sens du Code de la Propriété Intellectuelle d'un quelconque droit de propriété intellectuelle au bénéfice de l'autre Partie.

Chaque Partie conserve la propriété entière et exclusive de tout autre élément, et notamment, sans que cette liste soit limitative : document, donnée, information, savoir-faire, fichier, logiciel, interfaces, documentation annexe, marques, brevets, dessins et modèles, support notamment pour la Formation, œuvre de l'esprit qui pourraient être mis à disposition, communiqués ou accessible par l'autre Partie, quels que soient la forme, le langage, le support, la version, etc.

Chaque Partie s'interdit de modifier, reproduire, adapter, diffuser, utiliser, contrefaire, vendre, céder, publier ou conserver une œuvre de l'esprit (y compris document, information, savoir-faire, support de Formation, etc) sur laquelle l'autre Partie est Titulaire des Droits de Propriété Intellectuelle, sans autorisation expresse, préalable et spécifique du Titulaire. Seule la partie détenant les droits peut effectuer ces opérations, notamment, pour permettre une utilisation conforme de son œuvre.

Chaque Partie s'engage à faire respecter les droits de propriété intellectuelle de l'autre Partie à ses sous-traitants, personnels ou cocontractants.

Chaque Partie garantit qu'elle dispose des droits et/ou des autorisations nécessaires permettant de conclure la Convention. A ce titre, elle garantit l'autre contre toute action en contrefaçon ou réclamation intentée à son encontre par un Tiers portant sur des droits de propriété intellectuelle de la Partie garantie exploités dans le cadre de l'exécution de la Convention par la Partie mise en cause.

Chaque Partie (dite « garante ») garantit l'autre contre toute action née d'une violation par ses salariés, sous-traitant(s) ou préposé(s) autorisé(s) par elle des dispositions légales et contractuelles ainsi qu'aux règles en vigueur applicables à la convention.

Chaque Partie s'engage à informer l'autre de tout fait susceptible de porter atteinte aux droits et éléments de la propriété intellectuelle visés aux présentes dont elle aurait connaissance au cours de l'exécution de celles-ci.

10 Conditions de résiliation

10.1 Résiliation à l'initiative de la DGFiP

La DGFiP peut mettre fin à la convention de Télétransmission, à son initiative en dehors de tout manquement des obligations par l'une des parties.

Dans cette hypothèse, la DGFiP souhaitant résilier l'accord-cadre s'oblige à notifier SITIV, par lettre recommandée avec accusé de réception moyennant le respect d'un préavis d'un (1) an précédant la résiliation.

La résiliation de l'accord-cadre prendra effet le lendemain du premier anniversaire de la réception de la LRAR, sauf si l'une ou l'autre des Parties en dispose autrement.

Dans cette hypothèse, SITIV s'engage à informer les Structures mandantes de la résiliation du présent Accord-Cadre.

Cette résiliation aura pour effet de retirer le droit à SITIV de télétransmettre les données et documents des Structures vers le portail de l'ENSAP. De ce fait, les modalités de télétransmission de l'accord-cadre en application de la Convention de Partenariat entre la Structure et la DGFiP en vue de l'exposition de documents de rémunération sur le portail ENSAP sont déterminées par ces dernières.

10.2 Résiliation à l'initiative de SITIV

SITIV peut mettre fin à la convention de télétransmission avec la DGFiP avec un préavis d'1 an, par lettre recommandée avec accusé de réception, à son initiative en dehors de tout manquement des obligations par l'une des parties.

Cette résiliation aura pour effet de suspendre le droit de télétransmission de SITIV des données et documents pour l'ensemble des Structures l'ayant mandaté.

En cas de résiliation d'un mandat de télétransmission d'une Structure, celle-ci a pour effet de suspendre le droit de télétransmission de SITIV des données et documents concernant ladite Structure. SITIV s'engage à en informer la DGFiP dans les meilleurs délais avant la résiliation effective du mandat.

Les modalités d'exécution de la Convention liant la DGFiP à la Structure sont organisées par ces derniers.

10.3 Résiliation pour manquement aux obligations contractuelles

En cas de défaillance de l'une des parties, l'autre partie dispose d'une faculté de résiliation de la convention au terme d'une mise en demeure (par courrier recommandé avec accusé de réception) restée infructueuse dans un délai de 30 jours.

Dans l'intérêt des Structures clientes, les parties se rapprocheront afin de déterminer les modalités d'exécution des prestations de télétransmission en faveur des Structures.

Dans tous les cas de résiliation du présent Accord, les droits et obligations découlant des articles ci-après continueront à s'appliquer jusqu'à ce que leurs effets soient complètement exercés ou remplis :

- Article. Confidentialité
- Article. Obligations des Parties
- Article. Loi applicable – Règlement des litiges

En cas de résiliation, et quel qu'en soit la cause, chaque Partie doit remplir ses obligations contractées jusqu'à la date de prise d'effet de la résiliation y compris les Parties exclues en cas de défaillance.

11 Clauses

11.1 Durée

Le présent Accord entrera en vigueur au jour de la signature de la dernière Partie. Il est conclu pour une durée indéterminée.

11.2 Modification de la Convention

Toute modification du périmètre de la convention ne pourra être prise en compte qu'après demande de l'une ou l'autre des Parties, analyse des conséquences par l'ensemble des Parties et signature d'un avenant par les deux parties. Cet avenant devra déterminer notamment les modifications apportées à la convention d'origine, tant pour ce qui concerne la partie financière que la partie technique ou les modalités d'intervention.
Tout autre forme de modification est nulle et non avenue.
Il est expressément convenu entre les Parties qu'en cas de désaccord entre elles sur les stipulations ci-dessus, la convention initiale continuera à s'appliquer en l'état.
La convention représente la totalité et l'intégralité de l'accord intervenu entre les Parties et se substitue à tout accord antérieur listé dans la convention.

11.3 Intuitu Personae

La convention a été conclue *intuitu personae*, c'est-à-dire en considération de la personne et des compétences des Parties. Elle ne pourra, en aucun cas, faire l'objet d'une cession totale ou partielle, à titre onéreux ou gracieux, par l'une des Parties sans l'accord préalable et par écrit de l'autre Partie.

Les présentes dispositions expriment seules l'intégralité de l'accord intervenu entre la DGFiP et SITIV. Toute modification ultérieure, pour être valable, devra faire l'objet d'un avenant cosigné par les deux parties.

11.4 Droit applicable et juridiction compétente

Le présent accord est régi par le droit français.

En cas de litige découlant de l'exécution ou de l'interprétation du présent accord, les Parties s'engagent à rechercher une solution amiable.

A défaut d'une telle solution dans un délai de TROIS (3) mois, le litige sera porté devant la juridiction compétente.

A, Nantes le ……..……..……..

Pour la Direction générale des Finances publiques, le sous-directeur, responsable du département du programme de modernisation du service des retraites de l'État

Monsieur David KARLE

A, Vénissieux le 18 mars 2025

SITIV Représenté par son Directeur Général

M. Stéphane Vangheluwe

ANNEXE I – MANDAT STRUCTURE

12 Objet

Le présent Mandat a pour objet d'encadrer l'exécution de la prestation de télétransmission des données vers l'Espace Numérique Sécurisé de l'Agent Public réalisée par SITIV, tiers-émetteur, pour le compte de la Nom de la Structure.

13 Documents contractuels

Les pièces qui régissent l'exécution de la prestation objet du présent mandat sont par ordre de priorité :

- Les Conditions Générales de Vente de SITIV.
- La Convention de Télétransmission SITIV /Ensap et la Convention de partenariat entre la Structure et la Direction Générale des Finances Publiques en vue de l'exposition de documents de rémunération sur le portail ENSAP.
- Les dispositions contractuelles entre SITIV et la Structure (dénomination exacte à indiquer)
- Le cas échéant, la fiche descriptive de l'offre de SITIV
- Le Mandat de Télétransmission ENSAP en Annexe à la présente Convention.
- Offre financière signée par la Structure.

Commenté [NLP1]: Il s'agit de la commande de la Structure auprès de son éditeur pour la prestation de télétransmission à l'ENSAP

En cas de contradiction, notamment au sein d'un même document, la volonté des Parties sera recherchée.

14 Modalités d'exécution du mandat

La Structure, mandataire, donne mandat à l'éditeur SITIV, mandant, d'exécuter la prestation de télétransmission, dans les conditions précisées dans les dispositions contractuelles entre SITIV et la Structure (dénomination exacte à indiquer)et l'Accord-Cadre régissant la relation contractuelle entre SITIV et la DGFiP, sur les documents et données de rémunération des agents et personnels de la Structure, en son nom et pour son compte.

La Structure s'engage également à respecter les conditions de mises en œuvre de la prestation de télétransmission, notamment, l'article *(numéro à préciser)* des dispositions contractuelles entre SITIV et la Structure *(dénomination exacte à indiquer)*.

La durée de ce mandat est précisée dans l'offre financière signée par la Structure.

A, (Ville) le ……

(Nom de la Structure)
Représenté par son …

M./Mme (Nom du signataire)

A, (Ville) le ……

SITIV Représenté par son Directeur Général

M. (Nom du signataire)

Annexe II - Clauses de sous-traitance relatives au Règlement Général Européen sur la protection des données personnelles (RGPD)

15 Objet

Les présentes clauses complètent celles **des Conditions Générales de Coopération et/ou des Conditions Générales de Vente** et précisent les conditions dans lesquelles, SITIV en tant que sous-traitant éditeur, prestataire de service ou hébergeur, s'engage à effectuer des opérations de traitement de données à caractère personnel pour le compte d'un responsable de traitement.

Ces clauses sont établies entre :

- **Le « Responsable de Traitement »** mettant en œuvre des traitements de données à caractère personnel, ayant souscrit un contrat avec SITIV parmi les catégories de services détaillés *(indiquer la référence de la partie du contrat détaillant les services souscrits par la Structure).*

- **Le « Sous-traitant SITIV»**, réalisant pour le compte du Responsable de Traitement des services détaillés en (*référence susmentionnée à rappeler ici)* pour un traitement de données à caractère personnel.

Il est entendu que la Direction Générale des Finances Publiques agit en tant que co-traitant des données à caractère personnel avec le Responsable de Traitement dans le cadre de l'exposition des documents de paie de ses collaborateurs sur l'Espace Numérique Sécurisé de l'Agent Public. A ce titre, la DGFiP ne saurait être considérée comme Sous-Traitant Ultérieur de SITIV dans le cadre de la réalisation de la prestation.

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, la loi Informatique et Liberté du 6 janvier 1978 et le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018.

16 Catégories de service faisant l'objet de sous-traitance

Le Sous-traitant SITIV est autorisé à traiter pour le compte du Responsable de Traitement, les données à caractère personnel nécessaires pour fournir les services suivants :

- Prestation de service

17 Finalités des traitements

Le Responsable de Traitement sous-traite à SITIV la prestation de télétransmission des documents de paie de ses collaborateurs vers l'Espace Numérique Sécurisé de l'Agent Public (ENSAP) édité et géré par la Direction Générale des Finances Publiques.

Parmi les traitements mentionnés à l'article *(indiquer la référence de l'article du contrat détaillant les finalités du traitement)* des CGC ou CGV, les traitements nécessaires à SITIV pour rendre le service objet de la sous-traitance sont les suivants :

- Conservation des données hébergées,
- Traçabilité des équipements des systèmes et réseau,

18 Données à caractère personnel traitées

Les données à caractère personnel traitées par le sous-traitant SITIV pour rendre les services objets de la sous-traitance sont :

- Les documents de paie des collaborateurs de la Structure (données d'identification, données d'ordre économique et financier, INS, données diverses apparaissant sur un bulletin de paie, et les données limitativement énumérées par le décret ENSAP[1]).

19 Catégories de personnes concernées par les données traitées

Les catégories de personnes concernées par les données traitées sont :

- Les personnels des services du Responsable de Traitement.

1 Décret n° 2022-1446 du 21 novembre 2022 fixant les modalités d'utilisation du traitement automatisé de données à caractère personnel dénommé Espace numérique sécurisé des agents publics (ENSAP)

20 Informations nécessaires à l'exécution du service

Pour l'exécution du service objet du présent contrat, le Responsable de Traitement met à la disposition du sous-traitant SITIV les informations nécessaires suivantes :

- Le Délégué à la Protection des Données du Responsable de Traitement à contacter pour le traitement des incidents ayant un impact sur les données personnelles hébergées,
- L'éventualité d'un traitement de données sensibles par son Système d'Information, afin que le sous-traitant SITIV puisse mettre en œuvre les mesures organisationnelles et techniques nécessaires pour assurer leur sécurité.
- Les données objets de la prestation de télétransmission.

21 Obligations du sous-traitant SITIV vis-à-vis du Responsable de Traitement

Les obligations du Sous-Traitant SITIV vis-à-vis du Responsable de Traitement sont recensées à l'article *(indiquer la référence de l'article et de la partie du contrat détaillant les obligations)* des Conditions Générales de Coopération et/ou des Conditions Générales de Vente de SITIV.

22 Obligations du Responsable de Traitement vis-à-vis du Sous-traitant SITIV

Les obligations du Responsable de Traitement vis-à-vis du Sous-Traitant SITIV sont recensées à l'**article** *(indiquer la référence de l'article et de la partie du contrat détaillant les obligations)* des Conditions Générales de Coopération et/ou des Conditions Générales de Vente de SITIV.

Envoyé en préfecture le 26/05/2025
Reçu en préfecture le 26/05/2025
Publié le
ID : 069-256910183-20250523-CS_2025_05_4-DE