

**CAHIER DES CHARGES FONCTIONNEL ET TECHNIQUE**

**ACCORD-CADRE D'ACCOMPAGNEMENT NATIONAL DE FRANCE TRAVAIL  
DANS LE CADRE DE LA CREATION ET LA REVISION DE SA CONFORMITE AU  
REGIME GENERAL DE LA PROTECTION DES DONNEES (RGPD), AU REGLEMENT DE  
L'INTELLIGENCE ARTIFICIELLE (RIA) ET A L'HOMOLOGATION DES SYSTEMES  
D'INFORMATION (SI).**

**N° DE CONSULTATION : 017.25**

<b>1. PRESENTATION DE FRANCE TRAVAIL</b>	<b>4</b>
<b>2. CONTEXTE</b>	<b>4</b>
<b>3. OBJET DU MARCHE</b>	<b>7</b>
3.1. Libellé et description du marché	7
3.2. Périmètre du marché	8
3.2.1 SUR LE PLAN TERRITORIAL :	8
3.2.2. SUR LE PLAN FONCTIONNEL :	8
<b>4. VOLUMETRIE</b>	<b>8</b>
<b>5. DESCRIPTION DÉTAILLÉE DES PRESTATIONS ATTENDUES POUR LE LOT 1</b>	<b>9</b>
5.1. Objectif des prestations	9
5.1.1 Les AIPD (UO 1) :	9
5.1.2 Les AIDF et autres obligations du RIA (UO 2 et UO 3)	10
5.1.3 MISE A jour AIPD /AIDF (UO4)	13
5.1.4 Articulation entre AIPD et AIDF (UO 5) :	13
5.1.5 Suivi des plans d'actions (UO 6) – prestations forfaitaires	14
5.1.6 Durée de réalisation des AIPD/AIDF	14
5.2. Typologie des AIPD/AIDF	15
5.3. Appropriation de l'environnement France Travail et du métier commanditaire par le prestataire (UO7 et UO 8)	17
5.4. Moyens et compétences nécessaires	18
5.4.1 : Support pour la réalisation des AIPD / AIDF	18
5.4.2 Profil des intervenants	18
<b>6. DESCRIPTION DÉTAILLÉE DES PRESTATIONS ATTENDUES POUR LE LOT 2 :</b>	<b>21</b>
6.1. Objectif des prestations	21
6.1.1. PILOTAGE DE LA DEMARCHE D'HOMOLOGATION	21
6.1.2. ROLES CLES ET RESPONSABILITES	22
6.1.3. MODALITES DE FONCTIONNEMENT	23
6.1.4. IDENTIFICATION DU NIVEAU DE DEMARCHE D'HOMOLOGATION	23
6.1.5. DEROULEMENT DES DEMARCHES D'HOMOLOGATION	26
6.1.6. SUIVI ET RENOUVELLEMENT DES HOMOLOGATIONS	28
6.2. Modalités d'exécution des prestations	29
6.2.1. Pré requis	29
6.2.2. Contenu de la prestation	29
6.2.3. Durée de la prestation	30
6.2.4. Appropriation des notions essentielles à la réalisation d'une homologation par l'équipe France Travail en charge du projet/produit concerné par l'homologation (UO 4 et UO 5 ?)	31
6.3. Appropriation de l'environnement France Travail et du métier commanditaire par le prestataire	32

<b>6.4.</b>	<b>Moyens et compétences nécessaires</b>	<b>32</b>
<b>7.</b>	<b><i>Attentes particulières vis-à-vis du titulaire</i></b>	<b>34</b>
7.1	Devoir de conseil	34
7.2	Plan de progrès	34
7.3	Devoir d'information	34
<b>8</b>	<b><i>Modalités de pilotage et de suivi du marché</i></b>	<b>35</b>
<b>8.1</b>	<b>Interlocuteurs du titulaire auprès de France Travail</b>	<b>35</b>
<b>8.2</b>	<b>Interlocuteurs de France Travail auprès du titulaire</b>	<b>36</b>
<b>8.3</b>	<b>Instances de pilotage et de suivi</b>	<b>36</b>
<b>8.4</b>	<b>Éléments de reporting</b>	<b>37</b>
<b>9</b>	<b><i>Opérations de contrôle de l'EXÉCUTION et de la qualité des prestations</i></b>	<b>37</b>
<b>9.1</b>	<b>Contrôles à la charge du titulaire</b>	<b>37</b>
<b>9.2</b>	<b>Contrôles réalisés par France Travail</b>	<b>38</b>

## **1. PRESENTATION DE FRANCE TRAVAIL**

Acteur majeur du marché de l'emploi en France, France Travail est un établissement public administratif, doté de la personnalité morale et de l'autonomie financière, et soumis aux règles comptables applicables aux entreprises industrielles et commerciales. Son directeur général est nommé en conseil des ministres.

France Travail est administré par un conseil d'administration, son action s'appuie sur une direction générale, et une organisation déconcentrée.

Une convention pluriannuelle d'objectifs et de gestion conclue entre l'État, l'Unedic et France Travail, définit les objectifs assignés à France Travail au regard de la situation de l'emploi et des moyens prévisionnels qui lui sont alloués par l'Unedic et l'État.

En matière d'achat, France Travail est soumis aux dispositions du code de la commande publique.

En application de la loi n°2023-1196 du 18 décembre 2023 pour le plein emploi, Pôle emploi est devenu France Travail le 1er janvier 2024. Cette transformation, qui n'emporte pas la création d'une nouvelle personne morale, consiste en un changement de dénomination et un élargissement des missions de l'établissement au sein du réseau pour l'emploi mentionné à l'article L.5311-7 du code du travail.

En tant qu'opérateur, France Travail a pour mission d'accueillir, d'informer, d'orienter et d'accompagner les personnes à la recherche d'un emploi, d'une formation ou d'un conseil professionnel et de veiller à la continuité de leur parcours d'insertion sociale et professionnelle. Il prescrit toutes les actions utiles pour développer leurs compétences professionnelles et améliorer leur employabilité. Il favorise leur reclassement, leur promotion professionnelle, ainsi que leur mobilité géographique et professionnelle. France Travail aide et conseille les entreprises dans leurs recrutements, prospecte le marché du travail et a également pour mission de développer une expertise sur l'évolution des emplois et qualifications.

France Travail assure également un certain nombre de missions pour le compte du réseau pour l'emploi. Notamment, il met à disposition des outils et services numériques, des actions de développement des compétences au bénéfice des personnels des autres membres du réseau et assure une fonction de centrale d'achat et d'appui auprès de ce réseau.

Pour répondre aux besoins des territoires et accompagner les agences dans leurs missions, France Travail s'appuie sur des Directions Régionales (DR), au nombre de 18 selon le découpage administratif national, 1 région « France Travail Services », et 1 région « Direction Générale ».

## **2. CONTEXTE**

Huit ans après la mise en œuvre du RGPD, France Travail a mis en place une organisation des traitements de données personnelles en renforçant les équipes RGPD au niveau national et régional, en cartographiant les traitements de données personnelles et en réalisant l'instruction RGPD dès la conception des projets. La loi plein emploi du 18 décembre 2023 porte l'ambition d'une amélioration de l'accompagnement des demandeurs d'emploi et des entreprises grâce à l'implication collective et coordonnée de tous les acteurs du secteur de l'insertion et de l'emploi. Ce renforcement de la coopération entre tous les acteurs de l'emploi et de l'insertion réunis au sein du Réseau pour l'emploi implique une augmentation des échanges de données personnelles et génère donc une montée en charge de l'instruction

RGPD de nouveaux traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Ces traitements devront donc faire l'objet d'une analyse d'impact à la protection des données (AIPD) notamment pour s'assurer du renforcement des mesures de sécurisation de notre système d'informations et des modalités de transmission de ces échanges de données.

En complément, avec l'émergence du déploiement de l'intelligence artificielle, le règlement européen sur l'intelligence artificielle (RIA) impose plusieurs obligations. Les systèmes d'IA (SIA) doivent notamment être sûrs et respecter les droits fondamentaux. Les SIA à haut risque doivent faire l'objet d'analyse d'impact sur les droits fondamentaux. (AIDF). En 2025, France Travail a initié des travaux de cartographie de ses SIA et a formalisé une doctrine pour la mise en conformité de ces SIA.

Enfin, le dispositif d'homologation de notre système d'information va devoir se renforcer au regard des enjeux actuel et à venir.

Le présent marché a vocation à couvrir ces évolutions, à savoir :

- La réalisation de nouvelles AIPD ou AIDF ;
- La mise à jour d'AIPD ou AIDF existantes (créées dans le cadre de ce marché ou déjà existantes) ;
- L'optimisation du dispositif d'homologation de France Travail en cours de refonte afin d'établir la liste des systèmes à homologuer à la commission d'homologation
- Le suivi de la mise en œuvre des différents plans d'actions identifiés lors de la réalisation des AIPD ou AIDF

- **Sur le traitement des AIPD/AIDF.**

L'analyse d'impact relative à la protection des données (AIPD) et l'analyse d'impacts sur les droits fondamentaux (AIDF) sont des outils de responsabilisation des responsables de traitement et des outils de conformité qui permettent de garantir la protection des données et des droit fondamentaux. France Travail doit être en capacité de démontrer à tout moment que les principes du RGPD et du RIA sont respectés.

L'AIPD et l'AIDF sont donc des outils permettant de construire un traitement conforme au RGPD et au RIA.

Les plans d'actions de remédiation qui découlent de ces analyses nécessitent un suivi régulier et renforcé afin d'en vérifier la bonne réalisation notamment pour alerter le directeur général de France Travail en cas de difficultés.

Le présent marché a pour objet l'accompagnement de France Travail dans la réalisation et/ou la mise à jour de ses analyses d'impact conformément au RGPD au RIA et l'homologation du système d'information.

Avec l'entrée en vigueur de la loi plein emploi et l'ouverture du SI de France Travail au RPE, France Travail engage une transformation de son offre de service. Concrètement, il s'agira de mettre en commun des moyens physiques, tels que des tiers lieux ou des espaces de travail, des moyens numériques, comme l'accès aux outils et/ou données du SI plateforme France Travail, le partage d'indicateurs de pilotage et de tableaux de bord à destination des gouvernances nationales et territoriales. Enfin, des communs méthodologiques relatifs à l'accompagnement des demandeurs d'emploi, des entreprises, et à la montée en compétences des professionnels du réseau pour l'emploi seront élaborés dans une logique de co-construction avec les partenaires.

La démarche de mise en conformité de ses traitements s'accélère pour être aux rendez-vous imposés par la loi plein emploi.

La mise en œuvre progressive du règlement européen de l'intelligence artificielle (RIA) vient compléter nos obligations en matière de documentation de conformité à l'utilisation de l'IA. :

Ce que France Travail intègre dans la gestion en flux des AIPD/AIDF :

- Les évolutions du système d'information de France Travail peuvent donner lieu à une nouvelle AIPD et AIDF (si le traitement embarque un système d'IA à haut risque), pour les traitements où France Travail est responsable de traitement ou responsable de traitement conjoint.
- Les traitements nationaux et régionaux pour lesquels le besoin d'une AIPD et/ou d'une AIDF serait identifié.
- Mise à jour d'une AIPD/AIDF existante qui serait impactée par des évolutions métiers significatives.
- La revue régulière des AIPD/AIDF, imposée par la CNIL, afin de revisiter les risques présentés par le traitement pour les personnes.

La direction protection des données personnelles et de la conformité des systèmes d'information de France Travail identifie les traitements nécessitant la réalisation d'une AIPD ou d'une AIDF voire d'une homologation de son système d'information.

Cet exercice est réalisé en concertation avec les directions métiers, la direction DATA, la direction de l'IA, la Direction des Affaires Juridiques (DAJ), le RSSI, les sous-traitants intervenant dans le traitement le cas échéant et les autres responsables de traitements dans le cas d'une responsabilité conjointe pour les traitements nationaux, et en concertation avec les responsables protection des données de la région concernée pour les traitements régionaux.

- **Sur le dispositif d'homologation de sécurité des SI à France Travail**

L'homologation est une démarche de maîtrise des risques d'un système d'information. Elle est l'attestation formelle que les besoins de sécurité ont été identifiés et traités de manière que les risques résiduels soient maîtrisés et acceptables. Cette attestation, la décision d'homologation, est prononcée par l'autorité d'homologation (AH) et l'engage.

L'homologation de sécurité des systèmes d'information est un dispositif issu du Référentiel Général de Sécurité (RGS) créé par l'article 9 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.

Les conditions d'élaboration, d'approbation, de modification et de publication du RGS sont fixées par le décret n° 2010-112 du 2 février 2010.

Le RGS est un référentiel destiné à sécuriser les échanges électroniques de la sphère publique. Pour une autorité administrative, appliquer le RGS permet de garantir aux citoyens et autres administrations que le niveau de sécurité de ses systèmes d'information est bien adapté aux enjeux et aux risques et qu'il est harmonisé avec ceux de ses partenaires.

France Travail est concerné :

- Au titre des télé services informatiques mis à disposition de ses usagers,
- Au titre des échanges de données informatiques avec d'autres autorités administratives,

- En tant qu'opérateur de services essentiels (OSE) au titre de NIS 1 ou entité essentielle (EE) au titre de NIS 2.

Le cadre réglementaire a été étendu par le décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics.

Une autorité d'homologation a été instaurée à France Travail en février 2021 : la Direction Générale Adjointe en charge de la stratégie et des affaires institutionnelles (DGA-SAI) par décision n° 2021-65 du 17 février 2021. A la suite d'une réorganisation intervenue au 1<sup>er</sup> mai 2025 au sein de la Direction Générale de France Travail, l'autorité d'homologation est désormais la Direction Générale Adjointe en charge de la Gouvernance, Responsabilité et Sécurité (DGA-GRS).

L'homologation de sécurité lorsqu'elle est requise pour un traitement informatique, constitue, en principe, l'ultime étape avant sa mise en production. Il s'agit donc de traiter, dans toute la mesure du possible, les dossiers d'homologation sur le flux.

Cependant, un retard significatif s'est constitué au fil du temps dans la réalisation des traitements à homologuer. Un état des lieux sur le stock d'homologations à rattraper a donc été réalisé au cours de l'année 2023. Cet état des lieux sur le stock d'homologation est en cours d'actualisation et de priorisation.

Enfin, France Travail a mené une réflexion sur l'organisation à mettre en place pour consolider le dispositif d'homologation de sécurité à partir de l'étude de l'existant :

- Rattrapage du stock et gestion du flux,
- Acteurs, rôle et responsabilités,
- Critères de priorisation,
- Processus de traitement des dossiers d'homologation,
- Composition et fonctionnement de la commission d'homologation.

Une doctrine a donc été établie, elle décrit le processus, la méthodologie, les rôles et responsabilités, des modèles de documents et un outillage pour le suivi des plans d'action.

Le titulaire se conformera à cette doctrine concernant l'élaboration des dossiers d'homologation tant sur le traitement en flux que sur le rattrapage du stock (cf. chapitre sur le détail des prestations attendues pour le Lot 2).

### **3. OBJET DU MARCHE**

#### **3.1. LIBELLE ET DESCRIPTION DU MARCHE**

Le présent marché a pour objet l'accompagnement national et régional de France Travail en ce qui concerne la création et la révision de ses analyses d'impact sur la protection des données relatives aux évolutions du système d'informations de France Travail. (Lot 1)

Le présent marché a aussi pour objet l'accompagnement national et régional de France Travail en ce qui concerne la création et la révision de ses analyses d'impact sur les droits fondamentaux pour tous système d'IA nécessitant une analyse ainsi que les analyses techniques pour les autres cas d'usages qui ne seraient pas à hauts risques. (Lot 1)

Le marché prévoit en complément d'assurer le suivi et la bonne réalisation concertée avec la DGA TECH (ex DSI) et notamment son RSSI des plans d'actions issues des constats réalisés

dans les analyses et fuites potentielles et à la demande des autorités de contrôle (CNIL, IGAS, cour des comptes, etc.). (Lot 1)

Enfin le présent marché accompagnera la réalisation/construction des dossiers d'homologation du système d'information selon 2 modalités (simple et plus), ainsi que le suivi de ses actions complémentaires. (Lot 2)

### **3.2. PERIMETRE DU MARCHÉ**

#### **3.2.1 SUR LE PLAN TERRITORIAL :**

Le marché concerne l'ensemble des directions métiers de la Direction Générale de France Travail, la DGA TECH (ex DSI) et l'ensemble des directions régionales de France Travail (dont France Travail Service).

#### **3.2.2. SUR LE PLAN FONCTIONNEL :**

Le marché concerne :

- les traitements de données personnelles nécessitant une AIPD ;
- les systèmes d'IA (AIDF et autres obligations) ;
- les homologations des systèmes d'information mis en œuvre par France Travail ;
- le suivi des plans d'action relatifs aux traitements de données, à la conformité des SIA et de l'homologation des systèmes d'information de France Travail.

### **4. VOLUMETRIE**

- **Lot 1 : Création et mise à jour des analyses d'impacts sur la protection des données personnelles (AIPD) et la création d'analyses techniques et d'impacts (AIDF) du règlement de l'intelligence artificielle**

La volumétrie annuelle des AIPD et des AIDF est estimée entre 25 et 50 AIPD/AIDF par an. Au-delà de cette estimation annuelle, des besoins ponctuels pourraient nécessiter la réalisation d'AIPD ou d'AIDF supplémentaires notamment pour les AIPD et AIDF des traitements en régions.

Sur cette base, une planification des besoins en AIPD et AIDF sera effectuée chaque trimestre dans le train RGPD pour identifier et prioriser les AIPD et AIDF à réaliser sur les mois qui suivent par typologie et métiers.

En complément des prestations relatives à la réalisation AIPD/AIDF et au suivi des plans associées, le Titulaire pourra également intervenir sur la création de support de formation ou sensibilisation ainsi que sur la présentation de ces supports aux agents de France Travail concernés

#### A noter pour les régions :

Elles sont concernées par la démarche de mise en conformité. Toutefois, le nombre d'AIPD et d'AIDF à réaliser en propre par celles-ci représente une part très faible par rapport à la Direction Générale.

- **Lot 2 : Homologations de sécurité des systèmes d'information**

L'estimation annuelle du nombre de dossiers à homologuer est estimée entre 25 et 35 dossiers par an.



Comme sur le lot 1, en complément des prestations relatives à la réalisation des homologations, le Titulaire pourra également intervenir sur la création de support de formation ou sensibilisation ainsi que sur la présentation de ces supports aux agents de France Travail concernés

## 5. DESCRIPTION DÉTAILLÉE DES PRESTATIONS ATTENDUES POUR LE LOT 1

### 5.1. OBJECTIF DES PRESTATIONS

L'objectif de la prestation du premier lot est la réalisation des AIPD et AIDF d'un traitement de données personnelles ainsi que d'un système d'IA (SIA) qui y serait embarqué.

En complément la prestation assurera la bonne mise en œuvre des plans d'actions issue de nos constats documentés, des violations des données et des audits internes/externes Il devra à minima, respecter le découpage imposé par la CNIL s'agissant des AIPD des traitements de données à savoir :

#### 5.1.1 LES AIPD (UO 1) :

De manière générale, le RGPD indique, dans son considérant 90, *“une analyse d'impact relative à la protection des données devrait être effectuée par le responsable du traitement, préalablement au traitement, en vue d'évaluer la probabilité et la gravité particulières du risque élevé, compte tenu de la nature, de la portée, du contexte et des finalités du traitement et des sources du risque. Cette analyse d'impact devrait comprendre, notamment, les mesures, garanties et mécanismes envisagés pour atténuer ce risque, assurer la protection des données à caractère personnel et démontrer le respect du présent règlement.”*

L'AIPD se décompose en plusieurs parties :

- **Une phase de cadrage** : Cette partie est la plus structurante pour la bonne réussite de la documentation. Elle consiste à bien appréhender les projets à accompagner en s'entourant des opérationnels pour en déterminer les enjeux (finalités, catégories de données...). Une phase d'observation/appropriation sera obligatoire pour être en maîtrise du sujet à traiter. Le chef de projet métier aura un apport théorique du projet. Ce cadrage sera réalisé conjointement avec la direction protection des données personnelles et de la conformité des SI, les directions métiers, les juristes, les équipes du RSSI. Le cas échéant, les équipes du responsable conjoint seront également associées.
- **Une partie relative à la description détaillée du traitement** envisagé ou mis en œuvre sera réalisée. Cette partie comprend aussi bien les aspects techniques qu'opérationnels des opérations de traitements. Il est nécessaire de décrire le traitement dans son ensemble : sa nature, sa portée, ses finalités, les catégories de données personnelles concernées, les destinataires et les durées de conservation et finalement les supports des données. Cette description est basée sur les principes du RGPD. Pour rédiger cette partie il faut s'entourer de toutes les personnes nécessaires au bon déroulement dans une temporalité acceptable pour tous et définie par la méthode SAFE du train RGPD.
- **Une partie évaluation des mesures garantissant la proportionnalité** et la nécessité du traitement est à réaliser. Il s'agit d'une analyse juridique portant sur les grands principes du RGPD. (Finalités, base légale, données et durées de conservation, information et droits des personnes, analyse des contrats et des transferts hors UE, etc.). Cette partie sera de la responsabilité du prestataire et validée finalement par les juristes de France Travail. Un conseil juridique sera possible pour soutenir

l'organisation en place de France Travail : les juristes de France Travail valideront la pré analyse juridique réalisée par le prestataire.

- Une partie de nature plus technique, des risques sur la sécurité des données (diagnostic de la sécurité ou analyse de la sécurité (ISP), confidentialité, intégrité et disponibilité des données) ainsi que leurs impacts potentiels sur la vie privée, qui permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données. Cette partie nécessite une bonne connaissance du système d'information, donc la présence du RSSI, et de ses équipes, est requise pour être mené à bien. Il faudra identifier dans un premier temps l'ensemble des mesures de sécurité déjà mise en place au sein de France Travail puis dans un second temps déterminer les impacts potentiels que pourrait engendrer le traitement sur la vie privée des personnes concernées.
- **Un plan d'action clair et détaillé** doit être formalisé à partir des différentes évaluations des trois parties de l'AIPD. Pour être le plus efficace possible, le plan d'action doit aussi mentionner les personnes responsables de la mise en œuvre de chacune des actions identifiées, le niveau de criticité de ces actions et proposer un calendrier prévisionnel. Ce plan d'action sera suivi dans le temps par le prestataire avec le concours de la direction protection des données personnelles et de la conformité des systèmes d'information.
- Enfin, **des éléments de synthèse** portant sur les phases précédentes sont inscrites dans l'AIPD afin que le responsable de la sécurité des systèmes d'information (RSSI) et le délégué à la protection des données (DPD) puissent rédiger leur avis sur le traitement.
- La décision du responsable du traitement sur la mise en œuvre du traitement porté à son attention conclut l'AIPD. L'AIPD sera transmise au directeur général par la direction de la protection des données personnelles et de la conformité des SI. (Signature électronique)

Par nature une AIPD ou une AIDF est complexe à réaliser en raison de la nécessité d'évaluer les risques, de vérifier la proportionnalité du traitement et de trouver un équilibre entre vie privée et l'ensemble des droits fondamentaux et l'innovation, Cette documentation implique également une coordination de différents acteurs au sein de l'établissement ou en externe (sous-traitants, responsables conjoints).

### 5.1.2 LES AIDF ET AUTRES OBLIGATIONS DU RIA (UO 2 ET UO 3)

Le Règlement (UE) 2024/1689 sur l'intelligence artificielle, dit « Règlement sur l'IA » (RIA) est le premier cadre juridique général, obligatoire, horizontal et harmonisé au niveau d'un bloc régional pour réguler l'intelligence artificielle. Il établit un cadre harmonisé visant à garantir que les systèmes d'IA (SIA) mis sur le marché de l'Union européenne soient sûrs, transparents et respectueux des droits fondamentaux, tout en favorisant l'innovation responsable.

Le RIA propose une approche fondée sur les risques en classant les systèmes d'IA en quatre niveaux :

• **Risque inacceptable** : le RIA interdit un ensemble limité de pratiques contraires aux valeurs de l'Union européenne et aux droits fondamentaux.

• **Haut risque** : le RIA classe comme à « haut risque » (i) les systèmes d'IA qui sont des composants de sécurité de produits (ou des produits eux même) couverts par les législations de l'UE énumérés à l'Annexe I (ex : dispositifs médicaux, jouets, véhicules, etc.) et les systèmes d'IA relevant des huit domaines listés à l'Annexe III (biométrie, infrastructures critiques, éducation, emploi, services essentiels/publics, application de la loi, migration/asiles/frontières, justice/démocratie). Ces systèmes sont soumis à des exigences renforcées (gestion des risques, documentation technique, transparence envers les utilisateurs, journalisation, supervision humaine, évaluation de conformité, etc.)

• **Risque limité** : Concerne les systèmes d'IA qui soit(i) interagissent avec des personnes (ex : chatbot), (ii) réalisent de la reconnaissance d'émotions ou de la catégorisation biométriques, (iii) génèrent ou manipulent des contenus (deepfakes, images/sons/vidéos, texte)

• **Risque minimal ou nul** : pour tous les autres systèmes d'IA, le RIA ne prévoit pas d'obligation spécifique. Selon la Commission européenne, il s'agit de la très grande majorité des systèmes d'IA actuellement utilisés dans l'UE ou susceptibles de l'être.

Par ailleurs, le RIA régule également certains modèles d'IA, en particulier les modèles d'IA à usage général aussi appelés "modèles de fondation" (ex. GPT-4, Claude, LLaMA, etc...). Ces modèles se définissent par leur capacité générale à servir une grande variété de tâches et à être intégré dans de nombreux systèmes d'IA ou applications à des fins multiples, avec ou sans adaptation.

Pour les SIA à haut risque, le RIA prévoit plusieurs niveaux d'obligation, allant de mesures de transparence et de documentation à une évaluation approfondie avec la mise en place de mesures d'atténuation des risques concernant les modèles d'IA à usage général à risques systémiques dont les capacités et l'utilisation attendue ou réelle pourraient avoir des effets négatifs significatifs sur le marché intérieur, notamment en raison de leur puissance : risques d'accidents majeurs, d'utilisation à mauvais escient pour lancer des cyberattaques, la propagation de biais préjudiciables (relatifs à l'appartenance ethnique ou au genre par exemple) et aux effets discriminatoires à l'encontre de certaines personnes, etc.

Dans ce cadre et afin de déterminer les obligations qui lui sont applicables, France Travail est tenue de recenser tous les cas d'usage recourant aux technologies d'IA et de décrire les principales caractéristiques de chacun de ces cas d'usages.

Dans certains cas, l'article 27 du RIA impose la réalisation d'analyses d'impact sur les droits fondamentaux (AIDF). S'agissant du règlement de l'intelligence artificielle, celui-ci impose plusieurs actions en fonction de la position dans laquelle se retrouve l'organisme.

**Dès lors que France Travail identifiera un système d'IA à haut risque, celui-ci nécessitera la réalisation d'une analyse d'impact sur les droits fondamentaux (AIDF).**

Une AIDF consiste à analyser l'impact potentiel d'un système d'IA sur les droits des personnes susceptibles d'être affectées par son fonctionnement. L'AIDF est une analyse des risques : elle ne vise pas à éliminer totalement les risques, mais plutôt à les identifier, à les évaluer et à les gérer efficacement. L'objectif d'une AIDF est d'identifier les risques pour les personnes concernées, d'évaluer leur probabilité et leur gravité, de proposer des mesures d'atténuation pour les contrôler, et enfin d'établir un plan complet pour garantir une gestion adéquate de ces risques. France travail en tant que déploreurs de SIA à haut risque doit réaliser des AIDF. Les AIDF doivent être réalisées avant de mettre en œuvre les systèmes d'IA.

L'article 27 du RIA définit un cadre global pour la réalisation d'analyses d'impact sur les droits fondamentaux (AIDF) dans le contexte des SIA à haut risque. Ce cadre vise à garantir que le déploiement de ces systèmes ne porte pas atteinte aux droits fondamentaux.

Cette analyse doit respecter plusieurs items :

- Le contexte de déploiement et l'objectif visé : une description précise et détaillée des processus dans lesquels le SIA à haut risque sera utilisé. Cela inclut une définition claire de l'objectif visé par le SIA dans son contexte opérationnel spécifique. La compréhension du contexte de déploiement est essentielle pour identifier les risques liés à l'utilisation du système
- Durée d'exploitation et fréquence d'utilisation : il s'agit de préciser la période et la fréquence auxquelles le SIA est destiné à être utilisé. Cela permet d'évaluer l'impact à long terme du système sur les droits fondamentaux et de s'assurer que l'analyse ne se limite pas à une perspective à court terme ;
- Les catégories de personnes physiques et les groupes susceptibles d'être concernés par son utilisation : Cela implique d'analyser le contexte spécifique dans lequel le système fonctionnera et d'identifier les personnes susceptibles d'être affectées par son déploiement ;
- Risques spécifiques susceptibles d'avoir une incidence sur les catégories de personnes physiques ou groupes de personnes identifiés : Il s'agit d'évaluer les effets néfastes potentiels, compte tenu des informations fournies par le fournisseur du système d'IA ;
- Mesures de contrôle humain : il faut décrire les mécanismes de contrôle qui seront mis en place, conformément à la notice d'utilisation, afin de garantir que le système fonctionne dans des limites sûres et éthiques ;
- Mesures d'atténuation des risques : La description des mesures à prendre en cas de matérialisation de ces risques doit être réalisée. Il s'agit notamment de dispositifs de gouvernance interne et de mécanismes de plainte internes, garantissant l'existence de procédures solides pour traiter tout problème survenant au cours de l'exploitation du système

**Par ailleurs en fonction de notre qualité de fournisseur ou deployeur nos obligations de documentations des SIA à haut risque sont aussi de notre responsabilité.**

La prestation sur ce champ devra réaliser les livrables incombant à France Travail en tant que :

- Déployeur de SIA à haut risque :

Pour chaque SIA HR, le titulaire du marché devra réaliser la rédaction des mentions d'information préalable, la formalisation de la procédure de gestion et de traitement des demandes d'explication des décisions individuelles, la définition des métriques de surveillance du modèle, etc.

- Fournisseur de SIA à haut risque :

Pour chaque SIA HR, le titulaire du marché devra identifier les risques connus et prévisibles, rédiger un plan de surveillance, documenter le cadre de gouvernance de données spécifique aux données utilisées pour entraîner/tester/valider le modèle composant le SIA HR, établir la documentation technique, documenter la journalisation du système, etc.

Comme pour les AIPD, pour chaque AIDF un plan d'action clair et détaillé doit être formalisé. Pour être le plus efficace possible, le plan d'action doit aussi mentionner les personnes responsables de la mise en œuvre de chacune des actions identifiées, le niveau de criticité de ces actions et proposer un calendrier prévisionnel. Ce plan d'action sera suivi dans le temps

par le prestataire avec le concours de la direction protection des données personnelles et de la sécurisation du système d'information.

Un suivi de la mise en œuvre des plans d'actions devra être assuré pour vérifier sa bonne réalisation et son suivi.

Une doctrine IA à France Travail a donc été établie fin décembre 2025, elle décrit le processus, la méthodologie, les rôles et responsabilités, des modèles de documents et un outillage pour le suivi des plans d'action.

Le titulaire se conformera à cette doctrine concernant l'élaboration des dossiers techniques et analyses d'impacts tant sur le traitement en flux que sur le rattrapage du stock.

Le titulaire de ce lot devra respecter les mêmes conditions que pour la réalisation des AIPD sur le volet RGPD.

### **5.1.3 MISE A JOUR AIPD /AIDF (UO4)**

France Travail considère une mise à jour d'AIPD/AIDF comme une révision d'une AIPD/AIDF existante n'entraînant pas de modification substantielle du traitement de données à caractère personnel ou système d'IA.

Seront considérées comme une mise à jour les modifications liées :

- aux fonctionnalités de ou des outils existants pour les finalités existantes ;
- à l'ajout de nouvelles données pour les finalités existantes,
- à la révision du contrat pour les sous-traitants existants ou sous-traitants existants ;
- à la révision d'une analyse de la sécurité (ISP ou diagnostic de sécurité) liée à l'AIPD initiale.

Ne seront pas concernés par une mise à jour les traitements existants avec :

- l'ajout d'une ou de plusieurs finalités (ou sous-finalité) ;
- L'ajout d'un nouveau sous-traitant (ou plusieurs) ou d'un sous-traitant ultérieur ;
- un nouvel outil interne ...

### **5.1.4 ARTICULATION ENTRE AIPD ET AIDF (UO 5) :**

Lorsqu'une AIPD et une AIDF seront à réaliser, le titulaire du marché devra proposer une articulation entre ces deux analyses. La démarche proposée devra être la plus efficiente. L'AIPD se concentre sur les risques liés à la vie privée et à la protection des données et l'AIDF sur les droits fondamentaux couvre un spectre plus large de préoccupations liées aux droits fondamentaux (dignité, égalité, libertés, justice ...). Par exemple, une AIPD réalisée en vertu du RGPD peut déjà couvrir certains aspects requis pour une AIDF, comme la protection des données ou les mesures de sécurité. Dans ce cas, l'AIDF vient compléter l'AIPD en abordant d'autres dimensions des droits fondamentaux, assurant ainsi une couverture complète sans duplication inutile. D'ailleurs, l'article 27, paragraphe 4, du RIA prévoit expressément cette possibilité : « Si l'une des obligations dans le présent article est déjà remplie par l'analyse d'impact relative à la protection des 8 données [...], l'analyse d'impact relative aux droits fondamentaux [...] complète l'analyse d'impact relative à la protection des données. »

### 5.1.5 SUIVI DES PLANS D' ACTIONS (UO 6) – PRESTATIONS FORFAITAIRES

La conformité des traitements RGPD et IA ne sont pas des actes ponctuels mais des processus d'amélioration continue visant à garantir, dans la durée, que les conditions de conformité définies lors des analyses initiales sont maintenues ou améliorées.

A ce titre, le titulaire doit accompagner la Direction Protection des Données Personnelles et de la Conformité des Systèmes d'Information (DPDPCSI) dans le suivi des plans d'actions issus de la réalisation des AIPD ou AIDF.

**L'(ou les) intervenant(s) du Titulaire qui assure(nt) ce suivi est (sont) d'un niveau Consultant Senior ou équivalent.**

Cette prestation est forfaitaire, cela étant à titre indicatif, France Travail estime qu'elle correspond à une mobilisation de 5 J/H par mois.

Chaque AIPD et AIDF doit donc faire l'objet d'un suivi des mesures de remédiation assurée par la DPDPCSI.

Les objectifs de ce suivi sont de :

- S'assurer que les plans d'actions issus des AIPD et des AIDF sont mis en œuvre et suivis dans les délais ;
- Garantir le suivi des évolutions (techniques, fonctionnelles, organisationnelles) et d'identifier les impacts potentiels sur les traitements de données personnelles.

Plus globalement ce suivi consistera à réaliser le suivi des actions de sécurisation de la donnée afin d'éclairer et alerter le comité directeur général et son directeur général d'éventuels alertes et arbitrages à prendre en matière de protection de la donnée et de cybersécurité. Cette remontée sera réalisée hebdomadairement au comité directeur général.

Ce suivi concernera aussi les éventuelles demandes de la CNIL et aussi les plans d'actions issus des violations de données majeures.

Ce suivi devra être piloté et suivi par un profil sénior pour challenger les directions métiers porteuses de ces actions.

Il conviendra de mettre en place l'outil partagé qui permettra ce suivi.

### 5.1.6 DUREE DE REALISATION DES AIPD/AIDF

Chaque AIPD/AIDF fait l'objet d'une réunion de lancement, à laquelle devront être présents :

- Les représentants de France Travail (non exhaustif) : représentant direction protection des données personnelles et de la conformité des SI, représentant métier, juristes, RSIFab, etc. – à adapter selon les analyses).

Les représentants du Titulaire et les personnes identifiées par lui qui seront dédiées à la réalisation de la prestation.

En fonction de la nature des traitements faisant l'objet d'une AIPD ou d'une AIDF, le délai de réalisation de chaque AIPD ou AIDF sera identifié au cas par cas au plus tard lors de la réunion de lancement et validé avec la DPDP CSI, la direction métier et la DAJ.

La durée de réalisation dépend de la complexité du traitement, des ressources disponibles et de la priorisation du sujet par France Travail au regard de la sensibilité du traitement.

Les éléments de sortie de chaque réunion de lancement d'une AIPD seront :

Un calendrier de réalisation de l'AIPD/AIDF Une identification des principaux jalons (dates de livraison des différentes parties) de l'AIPD/AIDF permettant une présentation aux directions

concernés (DPDPCSI et RSSI et/ou métiers, IA, ...) pour validation définitive du calendrier proposé.

Ces éléments de sortie sont communiqués par le Titulaire dans un délai permettant d'arrêter un calendrier définitif dans un délai de deux semaines et au plus tard avant la réunion de lancement.

Le Titulaire veille à ce que la réalisation d'une AIPD/AIDF soit proportionnée et conforme aux échanges lors des cadrages et des réunions de lancement.

Cette obligation n'engage le Titulaire que dans la mesure où le retard lui est imputable malgré la communication par France Travail de l'ensemble des informations nécessaires à la réalisation de l'AIPD ou de l'AIDF.

## 5.2. TYPOLOGIE DES AIPD/AIDF

Les prestations qui pourront être demandées sont les suivantes :

Typologie	Particularité de la typologie
<b>UO1</b> <b>Création AIPD d'un traitement</b>	<ul style="list-style-type: none"><li>Analyse sécurité France Travail (diagnostic sécurité ou ISP) non existante</li><li>Description de la sous-traitance pour le traitement</li><li>Forte étendue des données traitées et aucune donnée sensible</li><li>Présence d'un algorithme</li><li>Analyse d'un processus de pseudonymisation ou d'anonymisation</li><li>Traitement en responsabilité conjointe avec un partenaire (au sens convention de partenariat et/ou titulaire de marché) de France Travail (<i>les traitements conjoints concerneront quasi exclusivement un seul partenaire en plus de France Travail</i>).</li><li>Données sensibles</li><li>Possibilité de saisine de la CNIL (décret à réaliser, données de santé, ...)</li><li>Enregistrement des éléments AIPD et de la fiche registre dans l'outil EQS</li></ul>
<b>UO2</b> <b>Création d'un dossier de sécurisation au RIA simplifié</b>	<ul style="list-style-type: none"><li>La documentation au RIA nécessite de rassembler les documentations techniques/éthique/RSE/juridique correspondant aux risques limité et risques minimal lorsque France Travail est déployeur ou fournisseur d'un SIA HR.</li></ul>

<p style="text-align: center;"><b>UO3</b> <b>Création d'une AIDF</b></p>	<ul style="list-style-type: none"> <li>• Systèmes d'IA qui sont des composants de sécurité de produits (ou des produits eux même) couverts par les législations de l'UE énumérés à l'Annexe I (ex : dispositifs médicaux, jouets, véhicules, etc.) et les systèmes d'IA relevant des huit domaines listés à l'Annexe III (biométrie, infrastructures critiques, éducation, emploi, services essentiels/publics, application de la loi, migration/asiles/frontières, justice/démocratie). Ces systèmes sont soumis à des exigences renforcées (gestion des risques, documentation technique, transparence envers les utilisateurs, journalisation, supervision humaine, évaluation de conformité, etc.)</li> <li>• Ces risques nécessitent la réalisation d'une AIDF (analyse d'impact sur les droits fondamentaux)</li> </ul>
<p style="text-align: center;"><b>UO4</b> <b>Mise à jour d'une AIPD OU AIDF existante</b></p>	<ul style="list-style-type: none"> <li>• Prise en compte des modifications liées : <ul style="list-style-type: none"> <li>• aux fonctionnalités de ou des outils (dont SIA) existants pour les finalités existantes ;</li> <li>• à l'ajout de nouvelles données pour les finalités existantes ;</li> <li>• à la révision du contrat pour les sous-traitants existants ou sous-traitants existants dans l'AIPD ou AIDF existante ;</li> <li>• À la révision d'une analyse de la sécurité (ISP ou diagnostic de sécurité) liée à l'AIPD initiale.</li> </ul> </li> <li>• Enregistrement des éléments dans l'outil EQS</li> </ul>
<p style="text-align: center;"><b>UO 5</b> <b>Création d'une AIPD à partir d'une AIDF ou création d'une AIDF à partir d'une AIPD</b></p>	<ul style="list-style-type: none"> <li>• Création d'une AIPD et d'une AIDF en quasi-simultané pour gagner en efficience en reprenant l'ensembles des points d'analyse d'une AIPD et d'une AIDF.</li> <li>• Mettre en place un process d'articulation entre ces deux analyses</li> <li>• Enregistrement des éléments dans l'outil EQS</li> </ul>
<p style="text-align: center;"><b>UO 6</b> <b>Suivi des plans d'actions</b></p>	<ul style="list-style-type: none"> <li>• Les plans d'actions issues des AIPD, des plaintes de la CNIL, des sanctions CNIL, des fuites de données, des plans internes devront faire l'objet d'un suivi régulier pour une remontée hebdomadaire à la direction protection des données.</li> <li>• Ce suivi de la mise en œuvre et de la bonne réalisation devra faire l'objet d'un reporting régulier et d'une compilation dans un outil adapté à ce suivi.</li> </ul>



<p><b>UO7</b></p> <p><b>Mise à disposition module de formation/sensibilisation/doctrine</b></p>	<ul style="list-style-type: none"> <li>• Construction de module de formation/sensibilisation/doctrine sur le sujet de la protection des données et RIA</li> </ul>
<p><b>UO8</b></p> <p><b>Animation/présentation doctrine sur la protection des données et RIA</b></p>	<ul style="list-style-type: none"> <li>• Animation et accompagnement sur des éléments de doctrine, sensibilisation/acculturation au sujet de la protection des données personnelles et RIA.</li> </ul>

### 5.3. APPROPRIATION DE L'ENVIRONNEMENT FRANCE TRAVAIL ET DU METIER COMMANDITAIRE PAR LE PRESTATAIRE (UO7 ET UO 8)

Afin de permettre une appropriation rapide de l'environnement de France Travail et du métier commanditaire de la prestation, une/des journées d'appropriations de cet environnement sera mise en œuvre lors de la première prestation commandée par la direction générale ou par une région.

Lors de cette prestation un corpus documentaire de référence sera remis au prestataire :

- Présentation de France Travail et de ses missions
- Documentation sur le métier concerné par l'AIPD ou AIDF
- Organigramme de la direction générale ou de la direction régionale commanditaire de la prestation
- Extrait du registre des traitements portant sur le domaine concerné par l'AIPD/AIDF
- Modèle d'AIPD/AIDF utilisé par France Travail.

Lors des commandes ultérieures de la direction générale ou par la région concernée, ce corpus documentaire sera communiqué lors de la réunion de lancement de la prestation de l'AIPD/AIDF visée.

#### Objectif :

Permettre aux agents de France Travail qui devront intervenir dans la réalisation d'une AIPD/AIDF d'identifier : leur rôle, leur intervention, leur taux d'investissement etc.

#### Public cible :

Agents mobilisés pour la réalisation d'une AIPD/AIDF : agents des directions métiers, des maîtrises d'ouvrage et de la DGA TECH (ex DSI).

#### Module attendu (livrable) :

Un module de présentation unique pour toutes les AIPD/AIDF.

Tous les agents concernés par la réalisation d'une AIPD/AIDF devront pouvoir y accéder :

- En autonomie : consultation en ligne du module (sur un format e-learning) avant de débiter la réalisation de l'AIPD/AIDF (le titulaire prévoit donc que le module puisse être accessible à partir d'un accès intranet à France Travail, ce qui implique que pour le dit module, France Travail acquière des droits d'utilisation et peut réutiliser le contenu du module à sa convenance

suivant les droits définis à l'article « propriété intellectuelle » du contrat. Ce module devra durer un maximum de 30 minutes.

- Par une animation du titulaire : le commanditaire de l'AIPD/AIDF pourra demander des prestations d'animation de séances interactives avec les agents concernés par la prestation de réalisation d'AIPD/AIDF – Ces séances réuniront un groupe maximum de 10 personnes pour chaque présentation. L'animation est une unité d'œuvre complémentaire à l'achat du module. Le titulaire s'engage sur son animation et la plus-value de celle-ci dans son cadre de réponse, valant engagement contractuel. Ces animations se dérouleront sur une durée maximale d'une heure.

En réunion de lancement de chaque AIPD/AIDF, il sera indiqué au titulaire s'il lui appartient de prévoir l'animation de la présentation ou si les agents y accéderont par leurs propres moyens. Le titulaire est informé que les animations se réaliseront majoritairement à distance, sauf demande expresse de France Travail.

Contenu : Seules les notions de la réglementation relative au RGPD et au RIA ou de la doctrine France Travail mobilisées pour la réalisation d'AIDF/AIPD y seront abordées. Il sera contextualisé à l'environnement France Travail afin de faciliter la projection des agents dans les situations abordées.

Le module de présentation sera validé par la « Direction de la protection des données personnelles et de la conformité des systèmes d'information » de France Travail.

Le titulaire pourra être amené à modifier le contenu de ce module, sur demande de France Travail, en cas de mise-à-jour nécessaire.

## **5.4. MOYENS ET COMPETENCES NECESSAIRES**

### **5.4.1 : SUPPORT POUR LA REALISATION DES AIPD / AIDF**

France Travail utilise pour la réalisation des AIPD un document type largement inspiré du modèle de la CNIL (cf. document joint en annexe) auquel des descriptions textuelles et des schémas peuvent être ajoutés pour la clarté du propos. Cette trame peut faire l'objet de suggestion d'améliorations. L'outil utilisé pour l'enregistrement de la documentation est EQS (ex Data Legal Drive).

Concernant l'AIDF, il n'y a pas à ce jour de modèle disponible par la commission européenne ou autre autorité de contrôle. La méthodologie utilisée par le Titulaire pour la rédaction d'une AIDF est celle décrite et fournie en annexe de son cadre de réponse. Cette méthodologie, être ajustée par France Travail si nécessaire.

Pour la réalisation de l'AIPD/AIDF, le prestataire peut mobiliser par l'organisation de réunions :

- L'interlocuteur désigné par la direction de la protection des données personnelles et de la conformité des systèmes d'information ;
- Les interlocuteurs métiers qui lui ont été désignés ;
- l'interlocuteur désigné par la direction des affaires juridiques de France Travail ;
- Le RSI Fab ainsi que le représentant du RSSI qui lui sont désignés ;

### **5.4.2 PROFIL DES INTERVENANTS**

Le prestataire doit disposer d'une équipe d'intervenants répondant aux exigences minimales suivantes en matière de niveau de formation et d'expérience ainsi que de connaissances techniques et de l'éco système de France Travail. La parfaite maîtrise de la réglementation

relative aux données personnelles, au règlement de l'intelligence artificielle ainsi que du dispositif d'homologation du système d'information est indispensable ainsi que la maîtrise juridique des règlements seront impérative dans le cadre de la réalisation des prestations du Titulaire, **toutefois cela n'implique pas que ce dernier collabore avec un cabinet d'avocat.**

#### Niveau de formation et d'expérience :

Pour réaliser une AIPD conforme au RGPD et une AIDF conforme au RIA, il est essentiel de faire appel à des consultants disposant des expertises suivantes :

#### **Expertise juridique :**

- Maîtrise du RGPD et de la réglementation nationale en matière de protection des données ;
- Maîtrise du droit numérique avec une spécialisation sur les problématiques spécifiques à l'IA
- Maîtrise des clauses relatives aux contrats informatiques ;
- Maîtrise du RIA, de ses exigences et de ses implications pour les projets IA (détection et atténuation des biais potentiels dans les SIA, propriété intellectuelle appliquée aux créations générées par des SIA, ...) ;
- Capacité à évaluer la nécessité et la proportionnalité des traitements de données ;
- Capacité à conseiller sur la conformité RGPD et RIA en mode privacy by design ;
- Connaissance des obligations légales et des bonnes pratiques en matière de protection des données (délibérations CNIL, jurisprudence, normes émergentes en IA ...).

#### **Expertise technique :**

- Compétences en sécurité des systèmes d'information (SSI) ;
- Compétences sur les SIA pour avoir la capacité d'appréhender notamment l'exploitation et la modélisation des données ;
- Connaissance des technologies de traitement des données et des risques associés ;
- Capacité à identifier les mesures techniques et organisationnelles pour atténuer les risques.

#### **Expertise en gestion des risques :**

- Méthodologie pour identifier, évaluer et hiérarchiser les risques liés à la vie privée et à l'utilisation de l'intelligence artificielle ;
- Capacité à élaborer des plans d'action pour la gestion des risques ;
- Expérience dans la réalisation d'analyses d'impact et d'audits de conformité.

#### **Expertise en gouvernance des données :**

- Connaissance des processus métiers et des flux de données ;

- Capacité à impliquer les parties prenantes et à coordonner les actions nécessaires ;
- Expérience dans la mise en place de politiques et de procédures de protection des données ou de procédures liées à la mise en œuvre de SIA.

### **Expertise en communication et reporting :**

- Capacité à sensibiliser et former les équipes métier aux enjeux de la protection des données lors des différents ateliers de rédaction des AIPD ou AIDF ;
- Compétences en rédaction de documents clairs et compréhensibles pour les parties prenantes ;
- Capacité à communiquer clairement sur l'avancement de l'AIPD ou de l'AIDF, les résultats des AIPD et AIDF à la direction protection des données personnelles et de la conformité des SI et aux différentes parties prenantes aux analyses d'impact.

Ces expertises permettent de garantir des AIPD et AIDF complètes et efficaces, en identifiant les risques et en proposant des mesures adaptées pour assurer la conformité au RGPD et au RIA.

Le Titulaire devra pouvoir mobiliser rapidement une équipe de consultants experts sur le RGPD, RIA et sécurité informatique lorsqu'une commande est effectuée. Il fournit à France Travail une liste d'intervenants disposant des prérequis que France Travail validera. Si besoin, un entretien pourra être réalisé avec ces intervenants.

Il prévoit également un suivi particulièrement important au démarrage et est force de proposition pour l'optimisation de la réalisation des différentes prestations.

Dans le cadre de ce marché, le Titulaire prend son engagement contractuel par sa réponse au cadre de réponse, en se conformant aux attendus de France Travail en termes de qualification et de séniorité (niveaux d'expérience des profils) :

**Le Consultant « confirmé »** : il dispose d'une expérience de 3 ans minimum (périodes de stage et d'alternance non incluses) dans la fonction et/ou dans les métiers du conseil. Sous l'autorité du directeur de mission ou d'un manager/consultant senior, il est capable de mobiliser les outils méthodologiques nécessaires à la réalisation des activités qui lui sont confiées et peut produire en autonomie les différents travaux et livrables attendus ;

**Le Consultant « senior »** : dispose d'une expérience minimum de 5 ans dans la fonction et/ou dans les métiers du conseil, ainsi que d'une expérience de 5 ans minimum dans le domaine des AIPD/RGPD. Sous l'autorité du directeur de mission, il doit prendre des initiatives et assumer des responsabilités. Il doit être capable d'assurer la mise en œuvre effective des outils méthodologiques, la production des différents travaux et livrables attendus et d'apporter un conseil stratégique à forte valeur ajoutée à ses interlocuteurs.

**Le Manager** : il justifie d'une expérience de 5 à 10 ans dans la fonction et/ou dans les métiers du conseil, ainsi que d'une expérience de 5 ans minimum dans le domaine des AIPD/RGPD. Sous l'autorité du directeur de projet, il est l'interlocuteur opérationnel du client. Il est capable d'assurer le pilotage de la mission, de diriger une équipe de plusieurs consultants et d'apporter un conseil stratégique à forte valeur ajoutée à ses interlocuteurs ;

**Le Directeur de projet** : justifiant d'une expérience d'au moins 10 ans dans la fonction et/ou dans les métiers du conseil, ainsi que d'une expérience d'au moins 5 ans en management d'équipe et gestion de projet, il dispose d'un domaine d'excellence et/ou d'une connaissance

du secteur reconnue et valorisable. Il est capable d'assurer la supervision de plusieurs projets en simultané et d'apporter un conseil stratégique à forte valeur ajoutée à ses interlocuteurs ;

## **6. DESCRIPTION DÉTAILLÉE DES PRESTATIONS ATTENDUES POUR LE LOT 2 :**

### **6.1. OBJECTIF DES PRESTATIONS**

Les homologations de sécurité des SI sont pilotées au sein de France Travail par le « Département homologation de sécurité des systèmes d'information » ci-après dénommé « Equipe homologation » dans la suite du texte.

Le « Département homologation de sécurité des systèmes d'information » est rattaché à la « Direction de la protection des données personnelles et de la conformité des systèmes d'information » qui est la direction prescriptrice de ce marché.

Les prestations attendues ont pour objet d'assurer pour le compte du « Département homologation de sécurité des systèmes d'information » la réalisation et le suivi des homologations de sécurité des SI y compris des plans d'actions associés. A ce titre le titulaire vient en appui l'équipe homologation déjà existante (3 collaborateurs), celle-ci ayant en charge le pilotage des prestations réalisées par le titulaire.

#### **6.1.1. PILOTAGE DE LA DEMARCHE D'HOMOLOGATION**

L'homologation est une démarche portée par les responsables des systèmes d'information (les directions métiers en charge du projet/produit).

Ces derniers sont accompagnés par l'équipe homologation qui joue un rôle central de facilitateur et de garant du cadre méthodologique.

L'équipe homologation :

- Définit les procédures, modèles et outils associés à la doctrine ;
- Accompagne les responsables de systèmes d'information et les chefs de projets dans la conduite de la démarche ;
- Veille à la cohérence et à la qualité des dossiers d'homologation ;
- Alimente le registre des homologations et assure le suivi ;
- Suit la mise en œuvre des plans d'action.

**La responsabilité d'engager et de conduire la démarche incombe au porteur du système d'information (les directions métiers en charge du projet/produit).**

Ainsi :

- Lors de la phase de cadrage d'un projet, le chef de projet métier doit saisir l'équipe homologation afin d'initier le processus ;
- Le chef de projet métier appuyé par l'équipe homologation demeure le garant des éléments du dossier d'homologation et de leur présentation devant l'Autorité d'homologation (AH) ;
- L'équipe homologation et le RSSI interviennent en support et validation, mais la maîtrise du contenu et du calendrier est sous la responsabilité du projet/produit.

### 6.1.2. ROLES CLES ET RESPONSABILITES

Acteur	Rôle principal	Responsabilités clés
<b>Autorité d'homologation (AH)</b>	Décideur final	<ul style="list-style-type: none"> <li>• Prend la décision formelle d'homologation ou non</li> <li>• Accepte et engage sa responsabilité sur les risques résiduels identifiés</li> <li>• S'appuie sur les avis du RSSI et de l'équipe homologation pour fournir son avis</li> </ul>
<b>Équipe homologation</b>	Facilitateur pour les projets et pilote méthodologique	<ul style="list-style-type: none"> <li>• Fournit les guides, modèles et outils</li> <li>• Contrôle la complétude et conformité du dossier</li> <li>• Prépare les éléments nécessaires à la tenue d'une commission ainsi que de l'organisation des commissions.</li> <li>• Suit la mise en œuvre des plans d'action</li> </ul>
<b>RSSI et équipe sécurité</b>	Référent et garant de la cohérence SSI	<ul style="list-style-type: none"> <li>• Contrôle l'évaluation de la conformité SSI</li> <li>• Valide la classification du système et le niveau de la démarche d'homologation</li> <li>• Fournit un avis à l'AH</li> </ul>
<b>Métiers</b>	Représentants du projet	<ul style="list-style-type: none"> <li>• Pilotent la démarche</li> <li>• Évaluent les enjeux métiers et la criticité du système</li> <li>• Produisent les pièces du dossier</li> <li>• Présentent le dossier à l'AH</li> <li>• Assurent le suivi du plan d'actions</li> </ul>
<b>DSI / DGA Tech</b>		<ul style="list-style-type: none"> <li>• Produisent les pièces du dossier</li> <li>• Assurent la mise en œuvre des plans d'action</li> <li>• Maintiennent les conditions d'homologation dans la durée (suivi des écarts et incidents)</li> </ul>

### 6.1.3. MODALITES DE FONCTIONNEMENT

#### Registre central des homologations

Un registre centralisé des homologations est tenu par l'équipe homologation avec l'appui du RSSI. Ce registre recense pour chaque SI :

- Le type de démarche (légère ou renforcée) ;
- L'état d'avancement ;
- La décision, date de décision et la durée de validité ;
- La date de la dernière revue du plan d'actions avec l'équipe homologation.

#### Instances de pilotage

Deux niveaux de pilotage sont mis en place :

Instance	Composition	Fréquence	Objectifs
<b>Comité opérationnel d'homologation</b>	<ul style="list-style-type: none"><li>• RSSI</li><li>• Équipe homologation</li></ul>	Mensuel	<ul style="list-style-type: none"><li>• Suivre l'avancement des dossiers</li><li>• Identifier les points de blocage</li><li>• Prioriser les plans d'actions</li></ul>
<b>Comité stratégique</b>	<ul style="list-style-type: none"><li>• DGA Tech</li><li>• RSSI</li><li>• Directeur équipe homologation</li></ul>	Trimestriel	<ul style="list-style-type: none"><li>• Suivre les indicateurs d'homologation</li></ul>

#### Accompagnement des projets

L'équipe homologation assure l'accompagnement des projets à toutes les phases de la démarche. Elle validera chacune des étapes du processus.

Un guide pédagogique de l'homologation est également disponible pour favoriser la compréhension des enjeux, la montée en compétences et en autonomie des différents acteurs.

### 6.1.4. IDENTIFICATION DU NIVEAU DE DEMARCHE D'HOMOLOGATION

La démarche d'homologation est le processus qui permet de collecter, d'évaluer, d'émettre et de présenter à l'autorité un avis de sécurité. Cette démarche repose sur une approche proportionnée : le niveau d'effort à fournir doit être cohérent avec les enjeux associés au système.

Ainsi, on distinguera deux niveaux progressifs de démarches :

- Le **niveau simple** destiné aux systèmes d'information **peu ou pas critiques** pour France Travail ;

- Le **niveau plus** appliqué aux systèmes manipulant des **données sensibles** ou ayant une **importance critique** pour France Travail.

L'identification du niveau de démarche s'effectue dès le lancement du projet, ou a posteriori pour les systèmes déjà en production dans le cadre du plan de rattrapage du stock.

Cette étape constitue une clé d'entrée du processus d'homologation : elle oriente les acteurs vers le bon niveau d'exigence, précise les livrables attendus, et permet à l'équipe homologation d'adapter son accompagnement.

### **Principes d'évaluation**

L'évaluation du niveau de démarche adapté repose sur deux axes :

- La criticité qui mesure les impacts d'un éventuel incident de sécurité sur les missions de France Travail ;
- L'exposition qui évalue le degré d'ouverture du système.

Ces deux critères sont analysés lors d'une réunion de lancement, initiée par l'équipe projet, incluant l'équipe homologation, l'équipe SSI. Cette analyse est réalisée en complétant la partie métier du *Kit Diag*.

### **Évaluation de la criticité**

La criticité étudie la gravité des impacts qu'un incident de sécurité pourrait avoir pour France Travail : perte de disponibilité, d'intégrité ou de confidentialité.

Afin de rendre l'approche simple et pragmatique, un Kit Diag est à disposition des projets et leur permet, avec l'appui des équipes homologation et sécurité d'apprécier les impacts sous différents angles :

- Opérationnel ;
- Financier ;
- Politique ;
- Réputationnel ;
- Judiciaire ;
- Sur les usagers ;
- Sociétal.

Une échelle de niveaux d'impacts est mise à disposition permettant une homogénéité au sein de France Travail.

Pour déterminer le niveau de criticité du système, on s'aligne sur les impacts les plus forts :

- $D / I / C^* = 4$  : Criticité critique
- $D / I / C = 3$  : Criticité élevée
- $D / I / C = 2$  : Criticité modérée
- $D / I / C = 1$  : Criticité faible

\*D : Disponibilité I : Intégrité C : Confidentialité

### **Évaluation de l'exposition**



L'exposition mesure le niveau de vulnérabilité potentielle du système d'information vis-à-vis des menaces extérieures et intérieures.

Elle prend en compte à la fois :

- L'exposition technique : niveau d'ouverture réseau, interconnexions, accessibilité depuis Internet ou des tiers
- L'exposition systémique : rôle du système, effet de levier potentiel, dépendances d'autres systèmes

Niveau d'exposition	Description
<b>Faible</b>	Le système est isolé ou peu connecté. Aucun accès distant ou interconnexion externe. La compromission aurait un impact limité.
<b>Modérée</b>	Système interne avec interconnexions maîtrisées et accès restreints à un nombre limité d'utilisateurs France Travail
<b>Élevée</b>	Le système est exposé à Internet ou joue un rôle transverse dans le SI, dont la compromission aurait un effet large mais non immédiat sur les autres systèmes.
<b>Très élevée</b>	Le système est directement exposé à Internet ou constitue un point d'entrée ou pivot critique donnant un accès étendu à l'ensemble du SI. Une compromission de ce système se diffuserait rapidement et affecterait l'ensemble du SI

### **Matrice de décision**

La sélection du niveau de la démarche doit faire l'objet d'un consensus entre les participants à la réunion de lancement.

La matrice suivante vise à apporter une aide à la décision dans ce choix.

	<b>Exposition faible</b>	<b>Exposition modérée</b>	<b>Exposition élevée</b>	<b>Exposition Très élevée</b>
<b>Criticité faible</b>	Simple	Simple	Simple	Simple
<b>Criticité modérée</b>	Simple	Simple	Plus	Plus
<b>Criticité élevée</b>	Simple	Simple	Plus	Plus
<b>Criticité critique</b>	Plus	Plus	Plus	Plus

### **Validation du niveau de démarche**

Le niveau de démarche d'homologation doit être validé par le directeur de l'équipe homologation par retour de mail.

### **6.1.5. DEROULEMENT DES DEMARCHES D'HOMOLOGATION**

#### **Démarche d'homologation simple (UO 2)**

La démarche d'homologation simple est conçue pour les systèmes dont la criticité et l'exposition sont faibles à modérées.

Elle repose sur une logique de conformité aux exigences minimales et de responsabilisation du projet, sans recourir à une analyse de risques complète.

#### **Constitution du dossier**

Le projet constitue un dossier allégé, comprenant :

- La note de qualification / partie métier du Kit Diag,
- Un questionnaire sécurité sur le modèle adapté,
- L'AIPD si le SI traite de données à caractère personnel,
- Les rapports d'audits des tests automatisés,
- Le plan d'actions cybersécurité identifiant clairement les responsables et échéances sur chaque action,
- Une proposition de décision d'homologation,
- La liste des incidents de sécurité.

#### **Analyse par l'équipe homologation**

L'équipe homologation réalise une revue de conformité du dossier et s'assure du respect méthodologique de la démarche.

Elle retourne le dossier au projet avec ses retours.

#### **Soumission à l'autorité d'homologation**

Le projet adresse le dossier dont la conformité a été validée par l'équipe homologation à l'AH pour décision, par courriel. L'équipe homologation ainsi que le RSSI sont intégrés les échanges de courriels.

L'AH peut homologuer, homologuer sous conditions ou refuser l'homologation.

#### **Notification et archivage**

L'AH notifie par retour de courriel sa décision au responsable du SI, au RSSI et à l'équipe homologation, puis elle signe électroniquement la décision d'homologation. L'équipe homologation met à jour le registre central des homologations en conséquence.

#### **Démarche d'homologation plus (UO 3°)**

La démarche renforcée s'applique aux systèmes à criticité élevée et à exposition forte.. Elle vise à assurer une analyse approfondie des risques et une vérification complète et avancée des mesures de sécurités mises en œuvre.

#### **Constitution du dossier d'homologation complet**

Le dossier inclut :

- La note de qualification / partie métier du Kit Diag,
- L'analyse de risques cybersécurité,
- L'AIPD si le SI traite de données à caractère personnel,

- Les rapports d'audits (test d'intrusion, audit de configuration et éventuellement audit de code, audit d'architecture),
- Le plan d'actions cybersécurité identifiant clairement les responsables et échéances sur chaque action,
- Le support de commission d'homologation contenant la proposition de décision d'homologation,
- La liste des incidents de sécurité,
- L'avis formalisé de l'équipe homologation,
- L'avis formalisé de la SSI.

### **Examen du dossier**

L'équipe homologation réalise une revue approfondie du dossier et émet un avis technique et méthodologique.

Cet avis conditionne le passage en pré-commission d'homologation.

### **Pré-commission d'homologation**

La réunion de pré-commission est destinée à passer en revue tous les éléments du dossier d'homologation. L'autorité d'homologation ne participe pas à cette réunion, durant laquelle les aspects techniques seront abordés.

La proposition d'homologation sera également discutée lors de cette réunion ; l'objet étant de n'avoir plus aucun sujet de débat lors de la commission d'homologation et que toutes les interrogations aient été levées.

### **Commission d'homologation**

La commission d'homologation est la réunion au cours de laquelle le dossier est présenté à l'autorité d'homologation. Cette dernière a déjà été informée par l'équipe homologation de la situation. Le dossier est présenté par le projet selon un axe métier et non technique.

La proposition d'homologation vers laquelle ont convergés les membres de la pré-commission est présentée mais c'est bien l'autorité d'homologation qui, à l'issue des échanges, rend sa décision.

### **Notification et archivage**

La décision est communiquée officiellement aux parties prenantes par courriel. L'AH signe électroniquement la décision d'homologation. L'équipe homologation met à jour le registre central des homologations en conséquence.

### **Synthèse des pièces du dossier**

Pièces du dossier	Simple	Plus
<b>Note de qualification / partie métier du Kit Diag</b>	X	X
<b>Questionnaire sécurité sur le modèle adapté du Kit Diag</b>	X	
<b>Analyse de risques</b>		X

<b>AIPD</b>	Applicable si traitement de DCP	
<b>Rapports d'audits</b>	X (scans auto)	X
<b>Plan d'actions consolidé</b>	X	X
<b>Support de commission d'homologation</b>		X

#### **6.1.6. SUIVI ET RENOUVELLEMENT DES HOMOLOGATIONS**

L'homologation n'est pas un acte ponctuel mais un processus continu visant à garantir, dans la durée, que les conditions de sécurité définies lors de la décision initiale sont maintenues ou améliorées.

##### **Suivi de l'homologation**

Chaque système d'information homologué doit faire l'objet d'un suivi de sécurité assuré conjointement par le responsable de système, l'équipe homologation et le RSSI.

Les objectifs de ce suivi sont de :

- S'assurer que les plans d'actions issus de l'homologation sont mis en œuvre et suivis dans les délais ;
- Garantir le suivi des évolutions (techniques, fonctionnelles, organisationnelles) et d'identifier les impacts potentiels sur la sécurité.

Pour cela :

- Le plan d'actions constitue la base du suivi ; il est maintenu par le responsable de système d'information dans un fichier consolidé partagé avec l'équipe homologation ;
- L'équipe homologation assure une revue périodique de l'avancement tous les 6 mois pour les SI homologation simple, tous les 3 mois pour les SI homologation plus ;
- En cas d'incident majeur ou de changement significatif (évolution d'architecture, migration, changement d'environnement d'hébergement, etc.), une revue d'homologation exceptionnelle est déclenchée.

##### **Durée de validité et conditions du renouvellement**

La durée de validité d'une homologation est fixée à 3 ans maximum, conformément aux bonnes pratiques recommandées par l'ANSSI. Cette durée peut néanmoins être inférieure puisqu'elle dépend de la maturité de la sécurité du système d'information, des évolutions prévues et de son exposition aux sources de risques numériques.

Un renouvellement anticipé peut être exigé dans les cas suivants :

- Évolution majeure du système ou de son environnement d'exploitation ;
- Réévaluation du niveau de menace ou découverte d'une vulnérabilité critique ;
- Incident de sécurité significatif remettant en cause les conditions initiales d'homologation ;
- Fusion, externalisation ou réorganisation impactant les responsabilités SSI.

## **Gestion des écarts et des conditions d'homologation**

L'homologation peut être accordée sous conditions, c'est-à-dire même lorsque toutes les mesures du plan d'actions ne sont pas terminées. Cela implique néanmoins que :

- Toutes les actions doivent avoir un responsable et une échéance acceptable compte tenu du risque résiduel que leur non mise en place fait peser sur le système ;
- Le non-respect des conditions à échéance peut entraîner la suspension ou le retrait de l'homologation, sur décision de l'AH après avis du RSSI et de l'équipe homologation.

### **6.2. MODALITES D'EXECUTION DES PRESTATIONS**

Le traitement mis en œuvre par le titulaire dans le cadre du marché a pour caractéristiques :

- Finalité : réalisation d'homologations de sécurité des SI
- Nature des opérations à réaliser sur les données : mise en œuvre d'un annuaire des contacts pour la réalisation de la prestation
- Catégories de données personnelles traitées : nom, prénom, positionnement dans l'entreprise, rôle dans le déroulé de la prestation, coordonnées de contact
- Catégories de personnes dont on traite les données : agent de France Travail

#### **6.2.1. Pré requis**

Le titulaire a une obligation de confidentialité concernant les informations de toute nature auxquelles il aura accès pour la réalisation de la prestation.

Un conseil juridique sera possible pour soutenir l'organisation en place de France Travail : les juristes de France Travail valideront la pré analyse juridique réalisée par le titulaire.

Le titulaire a une bonne connaissance des missions et métiers de France Travail et de son environnement.

#### **6.2.2. Contenu de la prestation**

Dans le cadre de chacune des prestations de réalisation et de suivi des homologations de sécurité les actions suivantes seront réalisées :

##### ***a) Pilotage de la démarche***

Le titulaire assurera le pilotage des homologations de sécurité selon la démarche présentée au chapitre 6.1 du présent CCFT et selon les rôles et responsabilités établis dans la doctrine. Il tiendra à jour le registre central des homologations et contribuera à l'organisation des instances de pilotage (comités opérationnels et comités stratégiques). Il accompagnera les différents acteurs (notamment des directions métier) à toutes les phases de la démarche.

A cette fin, il organise, autant que de besoin, les réunions nécessaires à la mise en œuvre de la démarche avec les acteurs du métier, de la maîtrise d'ouvrage et de la DSI concernés par

le projet/produit sur la base d'une liste d'acteurs remise par le correspondant métier en charge du projet/produit.

***b) Identification du niveau de démarche (simple/plus)***

Le titulaire contribuera à l'évaluation du niveau de démarche à mettre en œuvre pour chacune des homologations dont il aura la charge en lien avec les autres acteurs concernés (métier / DSI / RSSI) et selon la méthode issue de la doctrine (cf matrice criticité / exposition aux risques). Mais France Travail décidera in fine du niveau de démarche.

***c) Déroulement de la démarche d'homologation***

Le titulaire assurera la constitution du dossier d'homologation selon le niveau de démarche retenu (simple/renforcé), il organisera les revues de conformité du dossier et s'assurera du respect méthodologique de la démarche. Il préparera la décision à soumettre à l'autorité d'homologation en lien avec les acteurs concernés (métier / DSI / RSSI). Dans le cas d'une démarche d'homologation renforcée, il organisera la pré-commission et la commission d'homologation, en rédigera les comptes-rendus (procès-verbaux). Il rédigera également la décision d'homologation selon l'avis rendu par l'autorité d'homologation et la soumettra pour signature et publication. Il procèdera à la mise à jour du registre central des homologations en conséquence.

***d) Suivi et renouvellement des homologations***

Le titulaire s'assurera que les plans d'actions issus de l'homologation sont mis en œuvre et suivis dans les délais. Le plan d'actions est maintenu dans un fichier consolidé partagé entre le métier, la DSI/RSSI et l'équipe homologation. Le titulaire assurera une revue périodique de l'avancement tous les 6 mois pour les SI homologation simple, tous les 3 mois pour les SI homologation renforcée. Le titulaire assurera également la surveillance des homologations arrivant à échéance en vue de leur renouvellement ou non. Le renouvellement obéit à la même démarche d'homologation que pour une homologation initiale.

### **6.2.3. Durée de la prestation**

Chaque homologation fait l'objet d'une réunion de lancement, à laquelle devront être présents :

- Les représentants de France Travail selon la matrice « Rôles et responsabilités » présentée précédemment.
- Les représentants du titulaire et les personnes identifiées par lui qui seront dédiées à la réalisation de la prestation.

Les éléments de sortie de chaque réunion de lancement d'une homologation seront :

- Un calendrier de réalisation de l'homologation
- Une identification des principaux jalons de l'homologation permettant une présentation aux différents acteurs concernés pour validation définitive du calendrier proposé.

Ces éléments de sortie sont communiqués par le titulaire dans un délai permettant d'arrêter un calendrier définitif sous deux semaines.

Le titulaire veillera à ce que la réalisation d'une homologation n'excède pas 6 semaines pour une homologation simple, 8 semaines pour une homologation renforcée, à compter de la validation du calendrier prévisionnel.

Cette obligation n'engage le titulaire que dans la mesure où le retard lui est imputable malgré la communication par France Travail de l'ensemble des informations nécessaires à la réalisation de l'homologation.

Pour ce qui concerne la reprise du stock d'homologations en retard, des critères de priorisation ont déjà été établis.

#### **6.2.4. Appropriation des notions essentielles à la réalisation d'une homologation par l'équipe France Travail en charge du projet/produit concerné par l'homologation (UO 4 et UO 5 ?)**

##### Objectif :

Permettre aux agents de France Travail qui devront intervenir dans la réalisation d'une homologation d'identifier : leur rôle, leur intervention, leur taux d'investissement etc.

##### Public cible :

Agents mobilisés pour la réalisation d'une homologation : agents des directions métiers, des maîtrises d'ouvrage et de la DSI.

##### Module attendu :

Un module de présentation unique pour toutes les homologations.

Tous les agents concernés par la réalisation d'une homologation devront pouvoir y accéder :

- En autonomie : consultation en ligne du module (sur un format e-learning) avant de débiter la réalisation de l'homologation (le titulaire prévoit donc que le module puisse être accessible à partir d'un accès intranet à France Travail, ce qui implique que pour le dit module, France Travail acquière des droits d'utilisation et peut réutiliser le contenu du module à sa convenance suivant les droits définis à l'article « propriété intellectuelle » du contrat. Ce module devra durer un maximum de 30 minutes.
- Par une animation du titulaire : le commanditaire de l'homologation pourra demander des prestations d'animation de séances interactives avec les agents concernés par la prestation d'homologation – Ces séances réuniront un groupe maximum de 10 personnes pour chaque présentation. L'animation est une unité d'œuvre complémentaire à l'achat du module. Le titulaire s'engage sur son animation et la plus-value de celle-ci dans son cadre de réponse, valant engagement contractuel. Ces animations se dérouleront sur une durée maximale d'une heure.

En réunion de lancement de chaque homologation, il sera indiqué au titulaire s'il lui appartient de prévoir l'animation de la présentation ou si les agents y accéderont par leurs propres moyens.

Le titulaire est informé que les animations se réaliseront majoritairement à distance, sauf demande expresse de France Travail.

Contenu : Seules les notions de la réglementation relative à l'homologation de sécurité des SI ou de la doctrine France Travail mobilisées pour la réalisation d'une homologation y seront abordées. Il sera contextualisé à l'environnement France Travail afin de faciliter la projection des agents dans les situations abordées.

Le module de présentation sera validé par la « Direction de la protection des données personnelles et de la conformité des systèmes d'information » de France Travail.

Le titulaire pourra être amené à modifier le contenu de ce module, sur demande de France Travail, en cas de mise-à-jour nécessaire.

### **6.3. APPROPRIATION DE L'ENVIRONNEMENT FRANCE TRAVAIL ET DU METIER COMMANDITAIRE PAR LE PRESTATAIRE**

Afin de permettre une appropriation rapide de l'environnement de France Travail et du métier commanditaire de la prestation, une journée d'appropriation de cet environnement sera mise en œuvre lors de la première prestation commandée par une direction générale adjointe ou par une région. Il convient de noter que les prestations commandées pour ce qui concerne les homologations de sécurité émanent actuellement presque exclusivement du niveau national. Cependant il n'est pas exclu qu'un projet/produit puisse être à l'initiative d'une région ; Lors de cette prestation un corpus documentaire de référence sera remis au titulaire :

- Présentation de France Travail et de ses missions
- Documentation sur le métier concerné par l'homologation
- Organigramme de la DG ou de la DR commanditaire de la prestation
- Support de présentation de la doctrine d'homologation au sein de France Travail
- Modèles de documents utilisés pour l'homologation.

Lors des commandes ultérieures de la direction générale adjointe ou par la région concernée, ce corpus documentaire sera communiqué lors de la réunion de lancement de la prestation de l'homologation visée.

### **6.4. MOYENS ET COMPETENCES NECESSAIRES**

#### **6.4.1 Matériel Documents utilisables et mobilisation des interlocuteurs France Travail**

France Travail utilise pour la réalisation des homologations de sécurité des SI des documents type et un outillage pour le suivi des plans d'actions.

Pour la réalisation de l'homologation, le titulaire peut mobiliser par l'organisation de réunions :

- Les interlocuteurs des directions métiers, de la maîtrise d'ouvrage et de la DSI qui lui ont été désignés
- Le représentant du RSSI qui lui est désigné
- Le chef du « Département homologation de sécurité des systèmes d'information » de France Travail ou l'un de ses collaborateurs.

#### **6.4.2 Profil des intervenants**



Le titulaire doit disposer d'une équipe d'intervenants répondant aux exigences minimales suivantes en matière de niveau de formation et d'expérience ainsi que de connaissances techniques et de l'éco système de France Travail.

Niveau de formation et d'expérience :

***Réglementation relative à l'homologation de sécurité des SI :***

Il est attendu du titulaire une bonne connaissance de la réglementation applicable en matière d'homologation de sécurité des SI, notamment :

- Du **Référentiel Général de Sécurité (RGS)** qui oblige à homologuer les SI considérés comme téléservices ou comportant des interconnexions avec des autorités administratives,
- Du **décret n°2022-513** du 8 avril 2022 qui étend, pour l'Etat et les établissements publics, l'obligation d'homologation à l'ensemble de leurs systèmes d'information et de communication,
- Du **Règlement Général sur la Protection des Données (RGPD)** qui exige de prouver la sécurité et la conformité des traitements de données personnelles : l'homologation est un moyen d'y répondre,
- De la **directive européenne NIS2** et sa transposition nationale qui introduit des exigences en matière de gestion des risques et qui responsabilise les dirigeants : l'homologation est un moyen d'y répondre,
- De la **Politique de Sécurité des Systèmes d'Information de l'État (PSSIE)** qui impose l'homologation de tous les SI de l'État.

Par ailleurs, le titulaire devra proposer des intervenants dotés de connaissances juridiques (même s'il n'est pas attendu de conseil juridique), qui lui permettront d'analyser les éventuels contrats de sous-traitance et conventions de partenariat en lien avec le projet/produit afin d'instruire le périmètre de responsabilité de France Travail et les garanties présentées par les parties prenantes au projet/produit.

***Analyse de risque et sécurité des SI :***

Il est attendu du titulaire une bonne connaissance des risques en matière de sécurité des systèmes d'information et de lutte contre la cybercriminalité.

***Connaissances techniques d'animation de projet :***

Il est attendu du titulaire une maîtrise des techniques d'entretien individuel et animation de groupes de travail ainsi que des compétences en gestion de projet.

Le titulaire devra pouvoir mobiliser rapidement une équipe de consultants lorsqu'une commande est effectuée.

Il prévoit également un suivi particulièrement important au démarrage et est force de proposition pour l'optimisation de la réalisation des différentes prestations.

Dans le cadre de ce marché, le titulaire s'engage contractuellement par sa réponse au cadre de réponse en se conformant aux attendus de France Travail en termes de qualification de séniorité :

Le **Consultant « confirmé »** : il dispose d'une expérience de 3 ans minimum (périodes de stage non incluses) dans la fonction et/ou dans les métiers du conseil. Sous l'autorité du directeur de mission ou d'un manager/consultant senior, il est capable de mobiliser les outils méthodologiques nécessaires à la réalisation des activités qui lui sont confiées et peut produire en autonomie les différents travaux et livrables attendus ;

Le **Consultants « senior »** : dispose d'une expérience minimum de 5 ans dans la fonction et/ou dans les métiers du conseil, ainsi que d'une expérience de 5 ans minimum dans le domaine des homologations de sécurité des SI. Sous l'autorité du directeur de mission, il doit prendre des initiatives et assumer des responsabilités. Il doit être capable d'assurer la mise en œuvre effective des outils méthodologiques, la production des différents travaux et livrables attendus et d'apporter un conseil stratégique à forte valeur ajoutée à ses interlocuteurs.

Le **Manager** : il justifie d'une expérience de 5 à 10 ans dans la fonction et/ou dans les métiers du conseil, ainsi que d'une expérience de 3 ans minimum dans le domaine des homologations de sécurité des SI. Sous l'autorité du directeur de projet, il est l'interlocuteur opérationnel du client. Il est capable d'assurer le pilotage de la mission, de diriger une équipe de plusieurs consultants et d'apporter un conseil stratégique à forte valeur ajoutée à ses interlocuteurs ;

Le **Directeur de projet** : justifiant d'une expérience d'au moins 10 ans dans la fonction et/ou dans les métiers du conseil, ainsi que d'une expérience d'au moins 5 ans en management d'équipe et gestion de projet, il dispose d'un domaine d'excellence et/ou d'une connaissance du secteur reconnue et valorisable. Il est capable d'assurer la supervision de plusieurs projets en simultané et d'apporter un conseil stratégique à forte valeur ajoutée à ses interlocuteurs ;

## **7. ATTENTES PARTICULIERES VIS-A-VIS DU TITULAIRE**

### **7.1 Devoir de conseil**

Le titulaire, du fait de son expertise, est tenu de conseiller France Travail sur les modalités d'exécution des prestations. Ce devoir de conseil s'exerce au fil de l'exécution des prestations : il peut porter sur l'organisation mise en œuvre, les modalités d'approvisionnement, plus spécifiquement sur tout point lié à l'objet du marché qui pourrait faire l'objet de propositions d'optimisation, et, de ce fait, à la réduction des coûts. Cela englobe aussi les éléments concernant la démarche environnementale qu'il est possible de mettre en place.

### **7.2 Plan de progrès**

De même, le titulaire s'engage à présenter à France Travail, annuellement, un plan de progrès dont l'objectif est l'optimisation des prestations.

### **7.3 Devoir d'information**

Le titulaire s'engage à informer ses interlocuteurs nationaux à la Direction Générale de France Travail de toute modification de la réglementation, de la norme en vigueur, de son processus de production, relative à la réglementation matière de protection des données ou à l'hygiène en matière de sécurité des systèmes d'information, relative à la réglementation en matière d'homologation de sécurité des SI ou à l'hygiène en matière de sécurité des systèmes d'information.

### **7.4 Clause carbone et respect de la loi « climat et résilience »**

L'exécution des prestations attendues doit s'insérer dans une démarche de protection ou de mise en valeur de l'environnement.

A cet effet, le titulaire s'engage pour l'exécution des prestations attendues à :

- Réduire le nombre d'impressions papier en généralisant le format électronique et en n'imprimant les documents que sur demande expresse de France Travail.

En cas d'impression papier, le titulaire utilise du papier recyclé et non blanchi ecolabellisé de type « Blue Angel » ou équivalent, en format recto-verso, avec une mise en page réduisant les impressions (2 documents par page, etc.) et une conception de document visant à limiter au maximum la consommation d'encre.

- Réduire et recycler les déchets notamment par le recours aux structures issues de l'économie circulaire spécialisées dans le ramassage, la valorisation et le recyclage des déchets).
- Réduire les déplacements professionnels en privilégiant le travail à distance.

A l'issue de chaque année d'exécution de marché, le titulaire présente à France Travail un bilan quantitatif et qualitatif des mesures ainsi mises en place.

## **8 MODALITES DE PILOTAGE ET DE SUIVI DU MARCHÉ**

### **8.1 INTERLOCUTEURS DU TITULAIRE AUPRES DE FRANCE TRAVAIL**

Le titulaire désigne dans sa proposition technique un représentant qui est l'interlocuteur privilégié de France Travail pour l'ensemble des questions contractuelles ; celui-ci a autorité pour régler toute difficulté liée à l'exécution des prestations. Il représente le titulaire dans toutes les réunions où celui-ci est convié dans le cadre de l'exécution du marché et du contrôle des prestations. Il est en lien avec l'acheteur qui assure le suivi de l'exécution contractuelle du marché à la Direction des achats de France Travail.

Le titulaire met également à disposition de France Travail une équipe dédiée pour traiter des questions liées à la gestion opérationnelle des prestations.

On distinguera les interlocuteurs en charge du marché et les interlocuteurs en charge de la prestation.

- Interlocuteurs en charge du marché :

DAM : lancement du marché et bilan annuel

- Interlocuteurs de la prestation relative à la réalisation d'une AIPD/AIDF ou d'une homologation de sécurité :

Direction Métier (nationale ou régionale) ou Moa du métier : lancement et suivi de la réalisation de l'AIPD ou de l'homologation de sécurité,

Pour ce qui concerne le suivi et les questions contractuelles relatives aux prestations, l'équipe dédiée du titulaire est en lien avec l'acheteur en charge du marché à la Direction des achats de France Travail.

## 8.2 INTERLOCUTEURS DE FRANCE TRAVAIL AUPRES DU TITULAIRE

Pour le marché cadre :

- Un représentant de chacune des DGA commanditaire d'achats de la prestation
- Le délégué à la protection des données de France Travail ou son représentant qui contrôle la conformité technique des prestations par rapport aux engagements du Titulaire dans son offre et au présent CCFT.
- Les représentants dédiés de la direction des achats-marchés : l'acheteur en charge du suivi de l'exécution contractuelle et le responsable du département achats ;

**Pour chacune des prestations du marché**, les interlocuteurs du titulaire au sein de France Travail pour la réalisation d'une AIPD ou d'une homologation de sécurité sont :

- Le directeur / la directrice de la direction commanditaire de l'achat de la prestation ou son représentant : interlocuteur métier et service gestionnaire du marché ;
- Les représentants dédiés de la direction des achats-marchés : l'acheteur en charge du suivi de l'exécution contractuelle et le responsable du département achats ;

## 8.3 INSTANCES DE PILOTAGE ET DE SUIVI

Pour le marché :

- Une **réunion de lancement** du marché réunissant les représentants du titulaire et les interlocuteurs nationaux de France Travail, cités à l'article 6.2
- Une **réunion trimestrielle** réunissant les représentants du titulaire et les interlocuteurs nationaux de France Travail, cités à l'article 6.2 pour l'identification, la priorisation et le lissage des prestations à réaliser dans les 6 prochains mois.
- Une **réunion de bilan annuel** permettant d'échanger sur l'exécution du marché et ses optimisations possibles, de partager les points d'alerte sur les difficultés éventuellement rencontrées ;
- Dans le cadre de la réalisation du marché, **des réunions peuvent être organisées ponctuellement** soit à la demande de France Travail, soit à la demande du titulaire

Pour chacune des prestations du marché :

- Une **réunion de lancement** de la prestation réunissant les représentants du titulaire et les interlocuteurs de France Travail, cités à l'article 8.2 ci-dessus, est organisée après la notification du marché par l'acheteur de la Direction Achats et Marchés.

Cette réunion a pour objectif de fixer le calendrier de mise en place du dispositif, les modalités opérationnelles d'exécution de la prestation et leur calendrier prévisionnel. Lors de la réunion de lancement, le représentant du titulaire doit être accompagné des personnes ayant la connaissance technique / chargés de l'exécution opérationnelle des prestations. Cette réunion de lancement a, en principe, lieu dans les 10 jours ouvrés suivant la notification du marché.

La réunion de lancement peut être suivie si besoin d'une réunion technique visant à définir les modalités opérationnelles de réalisation des prestations.

- Une **réunion de bilan** permet d'échanger sur l'exécution de la prestation et les optimisations possibles, partager les points d'alerte sur les difficultés éventuellement rencontrées ;

- Dans le cadre de la réalisation de la prestation attendue, **des réunions peuvent être organisées ponctuellement** soit à la demande de France Travail, soit à la demande du titulaire.
- Dans le cadre de la réalisation de la prestation attendue, **des réunions peuvent être organisées selon un calendrier défini conjointement en début de prestation.**

Les invitations aux réunions sont envoyées par mail. Les comptes-rendus des réunions sont établis par le titulaire, transmis à France Travail dans les 2 jours ouvrés qui suivent les réunions, et validés par lui.

Les réunions nécessaires à la réalisation des AIPD et des AIDF se tiendront prioritairement en présentielles pour les cadrages ainsi que les lancements des analyses et en distanciel dans ses phases de rédaction. Si l'AIPD ou l'AIDF concerne un traitement régional, la modalité distancielle sera privilégiée.

La même approche guidera l'accompagnement sur le dispositif d'homologation du système d'information.

Enfin l'accompagnement sur la mise en œuvre et le suivi des plans d'action privilégiera une modalité en fonction du contexte que les équipes rencontreront.

#### 8.4 ÉLÉMENTS DE REPORTING

Le titulaire fournit à France Travail, chaque trimestre calendaire les éléments suivants (données arrêtées au dernier jour de chaque période – 31 mars/30 juin/30 septembre/31 décembre) :

- *la liste des UO commandées sur le trimestre considéré*
- *la liste des AIPD AIDF ou Dossier de Sécurisation RIA simplifié planifiées sur le semestre à venir*
- *la liste des homologations de sécurité sur le semestre à venir*

L'ensemble doit être organisé par direction régionale (la DG est considérée comme la région « DG ») et direction métier commanditaire de la prestation.

Ces données sont transmises par mail à l'interlocuteur désigné de France Travail au plus tard dans les 10 jours calendaires du mois qui suit la période de référence.

De même, avant le 31 janvier de chaque année, le titulaire transmet à France Travail une consolidation annuelle (N-1) des mêmes éléments.

Les caractéristiques de cette interface sont décrites en annexe 2 du présent CCFT.

## 9 OPERATIONS DE CONTROLE DE L'EXÉCUTION ET DE LA QUALITE DES PRESTATIONS

### 9.1 CONTROLES A LA CHARGE DU TITULAIRE

Le titulaire veille à ce que les normes de qualité mises en œuvre pour l'exécution des prestations attendues soient appliquées sans défaut jusqu'au terme de la prestation dont il est responsable.

Il effectue tous les contrôles de cohérence nécessaires à la bonne réalisation des prestations attendues. Il soumet à France Travail détail des moyens mis en œuvre et lui fait connaître la procédure qualité activée. Cela comprend le contrôle des engagements environnementaux pris et la preuve de leur tenue tout au long du marché.

Il veille en particulier à la confidentialité des éléments recueillis au cours de la réalisation de l'AIPD ou de l'homologation de sécurité.

En cas d'incident, le titulaire fournit à France Travail les procédures ou actions correctives mises en œuvre.

## **9.2 CONTROLES REALISES PAR FRANCE TRAVAIL**

Afin de contrôler le respect des engagements contractuels, France Travail se réserve le droit de demander, en cours d'exécution du marché, toutes les informations qu'il jugerait utiles au suivi de l'exécution des prestations.

France Travail se réserve également la possibilité d'effectuer des contrôles de la qualité d'exécution des prestations, sur les lieux d'exécution du marché.

## ANNEXE I

Exemples de domaine et sous domaines du registre des traitements ou porteurs de projets/produits pouvant nécessiter des homologations de sécurité

### Domaine Offre de service

- Gestion de la liste
- Accueillir, échanger, communiquer
- Conseil et accompagnement vers l'emploi
- Formation des demandeurs d'emploi
- Gérer les droits à l'indemnisation et aux aides financières
- Service aux entreprises

### Domaine Ressources humaines

- Gestion administrative et traitement de la paie
- Gestion du temps et gestion du repos
- Développement RH, gestion de la formation et de la performance
- Relations sociales
- Infocentre interne
- Assistances

## **ANNEXE II**

La liste de reporting contient à minima les éléments suivants

- Région (dont DG)
- Direction commanditaire de l'AIPD ou de l'homologation de sécurité
- Date de lancement de la prestation (si la prestation prévoit plusieurs AIPD ou homologations de sécurité)
- Date de lancement de l'AIPD ou de l'homologation de sécurité
- Type d'Unité d'œuvre mise en œuvre pour la réalisation de l'AIPD ou de l'homologation de sécurité
- Date de finalisation de l'AIPD ou de l'homologation de sécurité