**Une image contenant texte, Police, capture d’écran, logo

Description générée automatiquementDélégation générale**

**à l’emploi et**

**à la formation professionnelle**

**Annexes au CCAP du lot 1**

**Clauses contractuelles types entre les responsables du traitement et les sous-traitants au titre de l’article 28 du règlement (UE) 2016/679**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Liste des parties et des acteurs

**Responsable de traitement**

Nom : Ministre chargée du travail, de la santé, des solidarités et des familles, représentée par le Délégué général à l’Emploi et à la Formation Professionnelle

Adresse : 14 avenue Duquesne 75 350 Paris 07 SP

Personnes habilitées à donner des instructions :

* Mathilde BONNETAIN : chargée de mission formation et insertion par l’activité économique (MIP/ SDPAE/ DGEFP) : [Mathilde.bonnetain@emploi.gouv.fr](mailto:Mathilde.bonnetain@emploi.gouv.fr)
* Louise FORNACCIARI : chargée de mission groupements d’employeurs pour l’insertion et la qualification (MIP/ SDPAE/ DGEFP) : [louise.fornacciari@emploi.gouv.fr](mailto:louise.fornacciari@emploi.gouv.fr)
* Guillaume SANSON : adjoint à la cheffe de la mission insertion professionnelle en charge de l’IAE (MIP/ SDPAE/ DGEFP) : [guillaume.sanson@emploi.gouv.fr](mailto:guillaume.sanson@emploi.gouv.fr)
* Philippine REGNIEZ cheffe de mission insertion professionnelle (MIP / SDPAE/ DGEFP) : [philippine.regniez@emploi.gouv.fr](mailto:philippine.regniez@emploi.gouv.fr)
* Marie BRUNAGEL cheffe de projets auprès de la sous-directrice des parcours d’accès à l’emploi (SDPAE/ DGEFP) : marie.brunagel@emploi.gouv.fr

Canal à utiliser (préciser : note, téléphone, mail, avenant…) : Courriel.

**Sous-traitant :**

Nom : …

Adresse : …

Personnes habilitées à recevoir les instructions : noms, fonctions, coordonnées

**(Option) Sous-traitant :**

Nom : …

Adresse : …

**Personnes habilitées à recevoir les instructions :** noms, fonctions, coordonnées

|  |  |  |
| --- | --- | --- |
| Responsable de traitement délégué : DGEFP |  | Sous-traitant : Nom de l’entité concernée |
| GOUVERNANCE DE LA SOUS-TRAITANCE | | |
| Mathilde Bonnetain   * mathilde.bonnetain@emploi.gouv.fr |  | Prénom Nom : Email :  Téléphone : |
| SUIVI OPERATIONNEL DU TRAITEMENT | | |
| Prénom Nom : Email :  Téléphone : |  | Prénom Nom : Email :  Téléphone : |
| SECURITE DES SYSTEMES D’INFORMATION | | |
| Prénom Nom : Boris SUPIOT  Email [boris.supiot@emploi.gouv.fr](mailto:boris.supiot@emploi.gouv.fr) |  | Prénom Nom :  Email :  Téléphone : |
| PROTECTION DES DONNEES PERSONNELLES (Référente RGPD) | | |
| Prénom Nom : Nadine Chasseigne  Email : dgefp.protectiondesdonnees@emploi.gouv.fr |  | Prénom Nom : Email :  Téléphone : |
| Autre | | |
| Prénom Nom : Email :  Téléphone : |  | Prénom Nom : Email :  Téléphone : |

### Description du traitement

Présentation du traitement faisant l’objet de la sous-traitance

**Contrôle de service fait des actions de formation financées dans le cadre du volet « insertion par l’activité économique » du plan d’investissement dans les compétences (PIC) 2024.**

La DGEFP, en tant que pouvoir adjudicateur du volet IAE des crédits du PIC tel que fixé par l’accord-cadre (2018-2022) prolongé en 2024 par avenant, a la charge d’évaluer ces programmes : elle agit par conséquent en qualité de responsable de traitement au sens du RGPD.

Ce contrôle de service fait porte notamment sur les actions de formations réalisées par les OPCO concernés.

**Catégories de personnes concernées dont les données à caractère personnel sont traitées**

Les personnes concernées sont les stagiaires des actions de formation financées par le PIC IAE.

**Catégories de données à caractère personnel traitées**

Les catégories de données concernées sont les données personnelles figurant sur le bulletin de salaire :

* Nom Prénom
* Date de naissance
* Bulletin de salaire
* Information sur le statut de travailleur handicapé le cas échéant.

Elles font l’objet d’une anonymisation avant traitement.

**Nature du traitement (opération)**

S’agissant des prestations à mener, les travaux et les unités d’œuvre sont précisés aux articles 3 à 4 du CCTP.

**Finalité(s) pour laquelle (lesquelles) les données à caractère personnel sont traitées pour le compte du responsable du traitement**

- Réaliser le contrôle de services fait des actions de formation financées par le PIC IAE.

L’accord-cadre se décompose en 4 phases comme suit :

* Phase n°1 : Lancement et mise en place des modalités de communication ;
* Phase n°2 : Contrôle de cohérence des bilans qualitatifs ;
* Phase n°3 : Contrôle sur échantillonnage des actions de formation ;
* Phase n°4 : Rapport de CSF par OPCO et rapport global.

Les phases n°2 et n°3 sont concernées par le traitement des données personnelles.

**Durée du traitement :**  Jusqu’à la fin de l’accord-cadre.

### Mesures techniques et organisationnelles, y compris mesures techniques et organisationnelles visant à garantir la sécurité des données

Description des mesures de sécurité techniques et organisationnelles mises en œuvre par le ou les sous-traitants visant à garantir un niveau de sécurité approprié, compte tenu de la nature, de la portée, du contexte et de la finalité du traitement, ainsi que des risques pour les droits et libertés des personnes physiques.

1. **Sécurisation des accès aux locaux et protection du matériel critique**

La protection des locaux et des équipements informatiques est essentielle pour garantir la confidentialité et l’intégrité des informations. Des mesures sont mises en place afin de limiter les risques d’accès non autorisés et de vol de matériel.

**Contrôle des accès physiques**

* Restriction des accès : Mise en place d’un contrôle d’accès (badges, serrures sécurisées) pour limiter l’entrée aux seules personnes autorisées ;
* Gestion des visiteurs : Enregistrement obligatoire des visiteurs et accompagnement dans les zones sensibles ;
* Surveillance et dissuasion : Utilisation de dispositifs de vidéosurveillance et d’alarmes pour détecter toute intrusion.

**Protection des équipements et des supports de données**

* Stockage sécurisé : Utilisation d’armoires verrouillées pour protéger les équipements critiques et les supports de stockage ;
* Suivi du matériel : Inventaire régulier des équipements et des supports contenant des données sensibles ;
* Destruction sécurisée : Mise en place de procédures de suppression définitive des supports obsolètes (broyeurs, effacement sécurisé).

1. **Sécurité du Réseau**

La mise en place de mesures de protection réseau vise à garantir l’intégrité et la confidentialité des échanges de données, en limitant les risques d’intrusion et d’interception.

**Contrôle des flux et protection périmétrique**

* Pare-feu et filtrage : Installation d’un pare-feu avec règles restrictives pour bloquer les connexions non autorisées.
* Surveillance des accès : Mise en place d’un système de journalisation permettant de détecter les anomalies et d’analyser les tentatives de connexion.

**Segmentation et isolation des services**

* Séparation des réseaux : Création de VLANs pour cloisonner les services internes, l’IoT et les ressources exposées.
* Protection des interfaces externes : Mise en place d’une DMZ pour sécuriser les services accessibles depuis l’extérieur, avec une configuration adaptée aux besoins métiers.

**Sécurisation des connexions à distance**

* Utilisation d’un VPN : Chiffrement des communications via une solution VPN SSL ou IPsec pour les accès distants.
* Authentification renforcée : Mise en place d’un double facteur d’authentification et de certificats pour les connexions aux ressources sensibles.

1. **Sécurité des Postes et Applications**

La sécurisation des terminaux et des applications est essentielle pour limiter les risques liés aux maliciels, aux vulnérabilités et aux accès non autorisés.

**Protection des équipements et des données**

* Détection et réponse aux menaces : Installation d’une solution EDR (Endpoint Detection and Response) et d’un antivirus/anti-malware régulièrement mis à jour.
* Filtrage des contenus : Mise en place d’une protection centralisée contre les menaces web et les emails malveillants.

**Gestion des mises à jour et des correctifs**

* Mise à jour automatisée : Application régulière des correctifs de sécurité sur les systèmes d’exploitation et les logiciels pour limiter les failles exploitables.

**Sécurisation des accès et des sessions**

* Politique de mots de passe robuste : Utilisation de mots de passe complexes et recours à un gestionnaire d’identifiants sécurisé.
* Authentification renforcée : Mise en place d’une authentification multi-facteurs (MFA) pour les comptes sensibles, notamment administrateurs.
* Verrouillage des sessions inactives : Configuration automatique pour limiter les risques d’accès non autorisés.

1. **Sécurité des Données**

La protection des données sensibles repose sur des mesures visant à garantir leur confidentialité, leur intégrité et leur disponibilité, tout en réduisant les risques de perte ou de fuite.

**Sauvegardes et restauration**

* Application de la règle « 3-2-1 » : Automatisation des sauvegardes sur plusieurs supports (local et cloud) avec vérifications régulières.
* Tests de restauration : Vérification périodique de l’efficacité des procédures de récupération des données.

**Contrôle des accès et anonymisation**

* Principe du moindre privilège : Attribution des droits d’accès strictement nécessaires, avec revue trimestrielle des autorisations.
* Réduction des risques en cas d’incident : Mise en place de l’anonymisation ou de la pseudonymisation des données sensibles lorsque cela est possible.

**Destruction sécurisée des données**

* Effacement définitif : Adoption d’une procédure d’effacement sécurisé et d’un calendrier de suppression automatique des données obsolètes.
* Traçabilité des destructions : Documentation des processus pour garantir leur conformité et leur suivi.

1. **Gouvernance et Conformité : Structurer la Sécurité et Sensibiliser les Équipes**

Une gouvernance efficace de la sécurité repose sur une organisation claire, une documentation actualisée et une culture de sensibilisation pour réduire les risques humains et garantir la conformité aux exigences réglementaires.

**Pilotage et organisation de la sécurité**

* Désignation d’un responsable de la sécurité : Identification d’un référent chargé de coordonner les actions de protection des systèmes d’information.
* Définition d’une politique de sécurité : Élaboration de règles internes adaptées aux risques et aux obligations légales.
* Gestion des incidents : Mise en place d’un processus de déclaration et de traitement des incidents de sécurité, avec une procédure d’escalade claire.

**Sensibilisation et formation continue**

* Intégration de la sécurité dès l’accueil : Formation initiale des nouveaux arrivants sur les bonnes pratiques et les risques numériques.
* Rappels réguliers : Campagnes de sensibilisation sur des thématiques clés (hameçonnage, protection des données, gestion des accès).
* Simulations et exercices : Organisation de tests (ex. : faux e-mails de phishing) pour évaluer et améliorer les réflexes de sécurité des équipes.

1. **Mesures Spécifiques**

* Contrôle d’Accès aux Données
  + Mise en place d’un système de gestion des droits d’accès renforcé, permettant un suivi précis des accès aux données sensibles.
* Sécurisation des Transferts et Stockage
  + Utilisation de protocoles sécurisés pour tous les transferts de données.
* Chiffrement systématique : Toute transmission de données sensibles doit être chiffrée, que ce soit via un canal sécurisé (TLS, VPN) ou au repos (fichiers protégés par chiffrement).

### Procès-verbal de destruction de données à caractère personnel et des informations confidentielles traitées

Je, soussigné, *…………………………………………………*, certifie que l’ensemble des données à caractère personnel et des informations confidentielles auxquelles j’ai eu accès dans le cadre de l’accord-cadre PRA023659 – Contrôle de service fait des dispositifs PIC IAE, FNE FORMATION, PRO A FORMATION dans le cadre du conventionnement entre l’Etat et les OPCO a été détruit de manière irréversible après l’avoir restitué intégralement à la Délégation générale à l’emploi et à la formation professionnelle en date du *Jour/Mois/Année*.

La destruction des données à caractère personnel a été réalisée à la date du *Jour/Mois/Année*.

Fait à

Le

Signature

### Notification d’une violation de données à caractère personnel et des informations confidentielles traitées

1. **Détection de l’incident de sécurité/violation de données**

**PRINCIPE**

Dès que le sous-traitant identifie ou est informé, par l'un de ses employés, par un système de détection, par des systèmes de gestion des événements et des informations de sécurité ou par toute autre source, d'une violation de données ou a des motifs raisonnables de soupçonner une telle violation, il doit immédiatement en informer le responsable désigné au sein de la DGEFP.

Les exemples ci-après sont des situations qui **déclenchent obligatoirement** l’application du présent mode opératoire :

* Un incident de sécurité est détecté via les outils d’analyse de logs ;
* Compromission d’un mot de passe d’une personne accédant aux données dans les environnements de production contenant des données à caractère personnel (ou tout autre environnement dès lors qu’il contient des données à caractère personnel) ;
* Perte d’un support (ordinateur, téléphone, clé USB, etc.) contenant des données à caractère personnel même si le support est chiffré ;
* Constat d’un accès illégitime à des données à caractère personnel ;
* Perte/suppression des données à caractère personnel ;
* Indisponibilité des données (uniquement liée à des incidents de sécurité) ;
* Constat d’une modification non désirée de données.

|  |
| --- |
| **Quel que soit le jour ou l’heure du constat de l’incident, celui-ci devra être notifié dans les plus brefs délais après en avoir pris connaissance.** |

|  |
| --- |
| **Le cas échéant, la notification de l’incident doit se faire concomitamment à la mise en place des mesures visant à stopper l’incident ou à en diminuer les conséquences probables (mesures de remédiation).** |

1. **Personne à notifier**

|  |
| --- |
| **Dans le cadre de la gestion des violations de données, il est nécessaire de connaître les bons interlocuteurs avec qui échanger et communiquer les bonnes informations. Cela est indispensable afin d’éviter tout manquement qui nuirait à un traitement efficace de la violation.** |

La liste des personnes à contacter au sein de la DGEFP, **quel que soit l’incident** :

1. La Sous-direction Europe et International de la DGEFP : [dgefp.sdei@emploi.gouv.fr](mailto:dgefp.sdei@emploi.gouv.fr)
2. Nadine CHASSEIGNE, Correspondante RGPD de la DGEFP : [nadine.chasseigne@emploi.gouv.fr](mailto:nadine.chasseigne@emploi.gouv.fr)
3. Boris SUPIOT, Sous-directeur de la Sous-direction du financement et de la modernisation, [boris.supiot@emploi.gouv.fr](mailto:boris.supiot@emploi.gouv.fr)
4. Le pôle RGPD [dgefp.protectiondesdonnees@emploi.gouv.fr](mailto:dgefp.protectiondesdonnees@emploi.gouv.fr)
5. **Formulaire de notification de violation de données**

*Partie à copier dans le corps d’un courriel*

|  |  |
| --- | --- |
| **Description l’incident de sécurité/violation de données** | |
| **Date de la violation** | |
| Date et heure du début de la violation/incident |  |
| Date et heure de la fin de la violation/incident |  |
| Date et heure de prise de connaissance de la violation/incident |  |
| Date et heure de notification de la DGEFP, et personne(s) notifiée(s) |  |
| Raisons du retard dans la notification de la DGEFP |  |
| Commentaires sur les dates |  |
|  | |
| **Contacts du sous-traitants** | |
| Les coordonnées des personnes en charge du traitement de l’incident et leur rôle[[1]](#footnote-2) |  |
| Les coordonnées du/de la Délégué(e) la Protection des données (DPO) du sous-traitant |  |
| Les coordonnées du Responsable de la Sécurité des Systèmes d’Information (RSSI) du sous-traitant |  |
|  | |
| **Information sur le système d’information concernés** | |
| Nom de l’application ou Système d’information concerné(e) |  |
| Environnement concernés (par exemple : production) et le nom de la base |  |
| Identité de l’organisme responsable de la base |  |
|  | |
| **A propos de la violation/incident** | |
| Toute information sur le statut de l’incident : terminé, en cours, analyse en cours, etc. |  |
| Circonstances détaillez de la découverte de la violation |  |
| La nature de l’incident (exemple : divulgation non autorisée de données, indisponibilité non intentionnelle du SI, extraction de données non autorisés, etc.) |  |
| Origine(s) de l'incident |  |
| Liste des données à caractère personnel concernées et/ou traitées dans l’application ou le SI |  |
| Données sensibles concernées |  |
| Nombre approximatif d'enregistrements concernés par la violation |  |
| Personnes ou catégories de personnes concernées (à qui appartiennent les données, exemple : salariés des entreprises) |  |
| Nombre approximatif de personnes concernées par la violation |  |
| La volumétrie des données impactées ou susceptibles d’être impactées par l’incident |  |
| Descriptif détaillé de la violation de données/incident |  |
|  | |
| **Information sur les mesures de sécurité** | |
| Mesures techniques et organisationnelles mises en œuvre préalablement à la détection de l’incident | *(Possibilité de joindre un document listant de manière détaillez les mesures techniques et organisationnelles de sécurité)* |
| Mesures techniques et organisationnelles mises en œuvre à compter de la détection de l’incident et celles en cours d’implémentation |  |
| L’existence d’une sauvegarde, et le cas échéant si elle est aussi impactée par l’incident |  |
| L’existence d’un Plan de Reprise d’Activité (PRA) et/ou un Plan de Continuité d’Activité (PCA) |  |
| Description de l’incident :   * Détection (qui, quand, comment) * Actions réalisées * Les analyses en cours et celles réalisées |  |
| Mesures techniques et organisationnelles de sécurité mise en place (au moment de la survenance de l’incident) susceptibles de réduire le risque pour les personnes en cas de violation de données |  |
|  | |
| **Autre** | |
| Autres informations jugées pertinentes |  |
| Liste des actions prises depuis la prise de connaissance de la violation/incident | 1 –  2 –  3 – |
| Document transmis à la DGEFP (date et heure) |  |
|  | |
| **Partie réservée à la DGEFP** | |
| Nom du PV clôture  (À saisir ultérieurement par la DGEFP) |  |

1. Dans la mesure du possible et en fonction de la gravité de la violation, toute information sur leurs contraintes personnelles, exemple : M. X doit impérativement aller chercher son enfant à l’école à 17h [↑](#footnote-ref-2)