|  |  |
| --- | --- |
| **Description : J:\DG-Commun\JURIDIQUE\UP_logo-texte.png** |  |

|  |  |
| --- | --- |
| **Objet du marché**  **Mise à disposition d’une solution de vote électronique infogérée**  **et prestations associées**  **Marché 2025UPHFS04VOT** | |
|  |  |

**ANNEXE B – DESCRIPTION DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL REALISE PAR LE SOUS-TRAITANT**

La présente annexe a pour but de définir les modalités pratiques de traitement des Données Personnelles que le sous-traitant s’engage à effectuer pour le compte du responsable de traitement.

1. **DESCRIPTION DES TRAITEMENTS FAISANT L’OBJET DE LA SOUS-TRAITANCE**

Le Sous-traitant accepte de réaliser le traitement dans les conditions de durée, de territoire, de type de données et de catégories de personnes concernées définies expressément par le Responsable de Traitement et reproduites ci-après.

1. **Responsable de traitement**

UPHF, Université Polytechnique Hauts de France, Campus Mont Houy, 59313 Valenciennes Cedex, SIREN 130025475.

Nom et coordonnées du Délégué à la protection des données (DPD): Camille DEMAN, [dpo@uphf.fr](mailto:dpo@uphf.fr), 03.27.51.11.33

INSA HdF Institut National des Sciences Appliquées, Hauts-de-France, Université Polytechnique Hauts de France, Campus Mont Houy, 59313 Valenciennes Cedex, SIREN 130025752

Nom et coordonnées du Délégué à la protection des données (DPD): Camille DEMAN, [dpo@uphf.fr](mailto:dpo@uphf.fr), 03.27.51.11.33

LAMIH, Université Polytechnique Hauts de France, Campus Mont Houy, 59313 Valenciennes Cedex

Nom et coordonnées du Délégué à la protection des données (DPD): Camille DEMAN, [dpo@uphf.fr](mailto:dpo@uphf.fr), 03.27.51.11.33

Autre : [compléter]

Nom et coordonnées du Délégué à la protection des données (DPD) ou Data Protection Officer (DPO): [compléter]

1. **Les finalités du traitement**

La ou les finalité(s) du traitement sont :

système de vote électronique par internet permettant d’organiser les élections suivantes :

* élections des représentants du personnel aux instances de représentation du personnel type Comité Social d’Administration et Commissions Paritaires ;
* élections des représentants du personnel et des étudiants aux conseils des établissements membres du groupement (Conseil d’Administration, Conseil de la Formation et de la Vie Etudiante, Conseil de la Recherche) et des conseils des composantes de formation et de recherche.

1. **Description des traitements réalisés**

Le Sous-Traitant est autorisé à traiter pour le compte du Responsable de traitement les Données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) définis par le Responsable de Traitement :

constitution de la liste des électeurs et regroupement par collèges et sous-collèges le cas échéant ;

enregistrement des candidats ;

Affichage de la liste électorale ;

Communication des informations de connexion aux votants ;

Connexion des votants ;

expression du suffrage selon les modalités prévues ;

dépouillement du vote et production automatique des résultats ;

archivage des données ;

destruction des archives selon les règles en vigueur.

participation à la cellule de supervision technique lors des scrutins prévue à l’article R. 211-522 du code général de la fonction publique.

1. **Nature des opérations**

La nature des opérations réalisées sur les Données est :

Lecture/consultation

Collecte (directe et indirecte)

Saisie

Enregistrement

Conservation

Modification

Rectification

Extraction

Diffusion/communication

Comparaison

Interconnexion

Limitation

Suppression

Destruction

\_\_\_\_\_\_\_\_\_\_

1. **Description des données à caractère personnel traitées**

|  |  |  |
| --- | --- | --- |
| **Données Personnelles**  *(liste exhaustive)* | **Personnes concernées** | **Durée de conservation** |
| Description des données  Matricule interne, Nom, prénom, adresse email professionnelle, adresse postale (si un envoi par courrier postal des identifiants a lieu), téléphone, question secrète, genre, date de naissance, ancienneté composante, collège, secteur ;  Données de connexion pour l’authentification : identifiant aléatoire transmis ou numéro d’identification interne puis mot de passe ;  Traçabilité des connexions (login, IP, identifiants navigateur et session) ; Registre d'activité horodaté ; Enregistrement du vote et de l’émargement dans chaque scrutin ;  Calcul des résultats issus des données de vote ;  Détail des listes électorales ou d’inscrits, détail des résolutions des candidats .  Données sensibles :  aucune,  origine raciale ou ethnique,  opinion politique,  croyance religieuse ou philosophique,  appartenance syndicale,  génétique ou biométrique,  santé,  vie sexuelle  Données particulières :  aucune condamnation pénale ou infraction,  NIR,  géolocalisation,  financière,  autre | Candidats  Etudiants  Doctorants  Famille/proches  Mineurs  Personnels BIATSS  Enseignant/Chercheur  Vacataire  Sujets d’études  Visiteurs  Fournisseurs  Partenaires  autre : candidats à l’élection, électeurs, membres du bureau et organisateurs | Description de la durée  Fin de période de recours électoral  Pour les purges régulières : suppression des données tous les \_\_\_\_\_\_\_\_\_\_.  Pour les purges ponctuelles : sur demande écrite et avec confirmation écrite de suppression. |

1. **LOCALISATION DES DONNÉES**

Le Sous-Traitant s’engage à ce que les Données soient localisées dans les conditions définies ci-après. Tout changement devra faire l’objet d’une notification au Responsable de traitement.

Le traitement des données implique un transfert ou un accès (même en lecture seule) des données dans les pays suivants :

France

UE : pays : \_\_\_\_\_\_\_\_\_\_\_\_

hors UE : pays : \_\_\_\_\_\_\_\_\_\_\_\_ - une Analyse d’impact du transfert de données est nécessaire

Transferts hors UE :

|  |  |  |
| --- | --- | --- |
| **Acteur** | **Pays** | **Mesure de protection retenue** *(Décision d’adéquation, Privacy Framework, Clause contractuelle Type de la Commission européenne, Clause contractuelle type de la CNIL, Binding Corporate Rules, Clauses autres que les clauses types avec autorisation de la CNIL, PIA)* |
|  |  |  |
|  |  |  |

1. **SOUS-TRAITANCE ET PARTENAIRES TIERS**

Le sous-traitant peut faire appel à des sous-traitants ultérieurs pour mener des activités de traitement spécifiques dans les conditions définies dans la présente annexe. Les sous-traitants déjà autorisés par le Responsable de traitement sont listés ci-dessous :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nom du sous-traitant ultérieur | Adresse du sous-traitant | Prestations sous-traitées | Durée de sous-traitance | Localisation des traitements | Sous-traitance en chaîne |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Le Sous-traitant devra déclarer tout autre sous-traitant ultérieur au Responsable de traitement.

1. **INFORMATIONS SUR LE SOUS-TRAITANT**

Nom et coordonnées du Délégué à la Protection des données ou Data Protection Officer (DPO) du sous-traitant ou assimilé : [compléter]

1. **INSTRUCTIONS FOURNIES PAR LE RESPONSABLE DE TRAITEMENT**

Les instructions sont :

Documentées dans les spécifications du traitement (initial et/ou d’évolution du traitement)

Inscrites dans l’outil de ticketing :

Reçues / confirmées à l’adresse suivante : \_\_\_\_\_\_\_\_\_\_

1. **DROIT D’INFORMATION DES PERSONNES CONCERNÉES**

Il appartient au responsable de traitement de fournir l’information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

Précisez les cas : de manière générale avant l’organisation des élections

Le Sous-Traitant, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l’information relative aux traitements de données qu’il réalise. La formulation et le format de l’information doit être définie par le responsable de traitement avant la collecte des données.

Précisez les cas : sur la plateforme de vote électronique pour les informations complémentaires demandées par la plateforme.

1. **GESTION DE L’EXERCICE DES DROITS DES PERSONNES CONCERNEES**

Les parties ont convenu d’un commun accord de suivre le process suivant concernant l’exercice des droits des personnes concernées :

Le Responsable de traitement n’autorise pas le Sous-Traitant à répondre directement.

Lorsque les personnes concernées exercent auprès du Sous-Traitant des demandes d’exercice de leurs droits, le Sous-Traitant doit adresser ces demandes dès réception au Responsable de traitement par courrier électronique à l’adresse [dpo@uphf.fr](mailto:dpo@uphf.fr) . Le Responsable de traitement donnera instruction ou non, par écrit, de répondre directement à la personne concernée. Dans le cas où le Responsable de traitement aurait transmis la demande au Sous-Traitant pour qu’il y réponde, ce dernier informera le Responsable de traitement, par écrit, de la réponse fournie et des suites de la demande.

1. **NOTIFICATION DES VIOLATIONS DE DONNEES A CARACTERE PERSONNEL**

En cas de notification de violations de Données à caractère personnel, le Sous-traitant respectera la procédure suivante :

☒ Le Sous-Traitant ne communique en aucun cas avec l’Autorité de contrôle compétente (CNIL)

☒ Le Sous-Traitant ne communique en aucun cas avec la personne concernée par la violation de Données à caractère personnel.

Le Sous-traitant communique la violation à l’adresse suivante du Responsable de traitement : [dpo@uphf.fr](mailto:dpo@uphf.fr)

1. **SORT DES DONNEES A CARACTERE PERSONNEL A L’ISSUE DU TRAITEMENT**

Au terme des Prestations relatives au traitement des Données, le Sous-Traitant s’engage, au choix du Responsable de Traitement, à :

Détruire toutes les données à caractère personnel dans un délai de 2 ans ou selon le délai de recours applicable à l’élection

Renvoyer, au format fichiers plats par un canal sécurisé, toutes les données à caractère personnel au responsable de traitement et notamment l’ensemble des supports nécessaires pour assurer un contrôle a posteriori des opérations : copies des codes sources et exécutables des programmes et du système sous-jacent, clés publiques de chiffrement, matériels de vote, fichiers de candidatures et professions de foi, fichiers d’émargement, de résultats, journaux d’évènements, fichiers de traçabilité, urnes et fichiers et PV des opérations électorales, sauvegardes, preuve mathématique, fragments de la clé de déchiffrement et code d’activation, fichier d’intervention sur le système.

Renvoyer, au format [SFTP, \_\_\_\_], les données à caractère personnel au sous-traitant désigné par le responsable de traitement dans un délai de \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Le renvoi doit s’accompagner de la destruction de toutes les copies existantes dans les systèmes d’information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par un Procès-Verbal de Suppression.

les conditions précises de Réversibilité sont définies dans un Plan de Réversibilité défini entre les Parties.

1. **MESURES MINIMALES DE SÉCURITÉ**

Dans la mesure où l’article 32 du règlement européen sur la protection des données prévoit que la mise en œuvre des mesures de sécurité incombe au responsable du traitement et au sous-traitant, il est recommandé de déterminer précisément les responsabilités de chacune des Parties au regard des mesures à mettre en œuvre.

Le sous-traitant s’engage à respecter et mettre en œuvre a minima la présente clause de sécurité.

**Le système de vote respecte les préconisations de la délibération CNIL n° 2019-053 du 25 avril 2019 portant adoption d’une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.**

**Le système de vote doit pouvoir répondre au niveau 3 de sécurité conformément à la délibération de la CNIL n°2019-053 du 25 avril 2019 portant adoption d’une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via internet.**

**Le système de vote sécurisé a fait l’objet d’une expertise indépendante conformément aux dispositions de la délibération CNIL n° 2019-053 du 25 avril 2019 précitée.**

**Le système de vote doit pouvoir répondre aux mesures de sécurité de l’ANSSI sur le vote électronique et au référentiel général de sécurité prévu à l'**[article 9 de l'ordonnance n° 2005-1516 du 8 décembre 2005](https://www.legifrance.gouv.fr/affichTexteArticle.do?cidTexte=JORFTEXT000000636232&idArticle=LEGIARTI000006317203&dateTexte=&categorieLien=cid)**relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives**

Mesures de protection des données pendant la transmission :

Les transferts de données sont effectués de la manière suivante :

FTPS

SFTP

VPN client/fournisseur/partenaire to site

VPN site to site

Filesender

Mesures visant à garantir la confidentialité, l’intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement :

pseudonymisation (remplacement de tout ou partie des données directement identifiants par un ID)

anonymisation (aucun moyen d’identifier directement l’individu, ni de savoir qu’un ensemble de données correspond à un individu unique)

chiffrement des données à caractère personnel

Mesures de protection des données pendant le stockage :

cloisonnement technique et applicatif des données

cloisonnement logique des données

Mesures visant à garantir la sécurité physique des lieux où les données à caractère personnel sont traitées :

Badges/cartes d’accès aux bâtiments

Badges/cartes d’accès, clé pour accéder aux locaux serveurs

Mesures d’identification et d’autorisation de l’utilisateur :

Politique de gestion des droits et des contrôles d’accès, et droits minimums

TOKEN de déverrouillage

Mots de passe robustes selon les dernières recommandations de la CNIL

Absence de compte anonyme ou partagé

Accès visiteur uniquement à un réseau internet hors réseau interne

Traçabilité des demandes de modification des droits (via tickets)

Mesures visant à garantir la configuration du système, notamment la configuration par défaut :

protection contre les codes malveillants

parefeu

antivirus mis à jour automatiquement et quotidiennement.

Scan en temps réel

Scan hebdomadaire programmé

Procédures visant à tester, à analyser et à évaluer régulièrement l’efficacité des mesures techniques et organisationnelles afin de garantir la sécurité du traitement

Scan de vulnérabilité

Test de pénétration

Audit de code

Mesures visant à garantir la journalisation des événements

journalisation des logs

Mesures pour la gouvernance et la gestion de l’informatique interne et de la sécurité informatique

mécanisme/procédure en cas de faille de sécurité

procédure de destruction ou de restitution des données

Une politique sur la sécurité de l’information

Une formation du personnel : sur la protection des données, sur les procédures et systèmes de sécurité.

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

plan de reprise et de continuité d’activités en cas de perte des données (PRA/PCA)

Back up et sauvegardes (archives) sur des lieux distincts

IRP (Incident Response Plan)

Mesures visant à garantir une conservation limitée des données

procédure de purge automatique des données tous les \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

procédure de purge automatique des données dans un délai fixé à l’issue du traitement : \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mesures de certification/assurance des processus et des produits

code de conduite, certification à mettre en œuvre les mesures de sécurité, ou adhésion à une norme reconnue sur la sécurité de l’information (ISO/IEC 27002).

assurance cyber sécurité