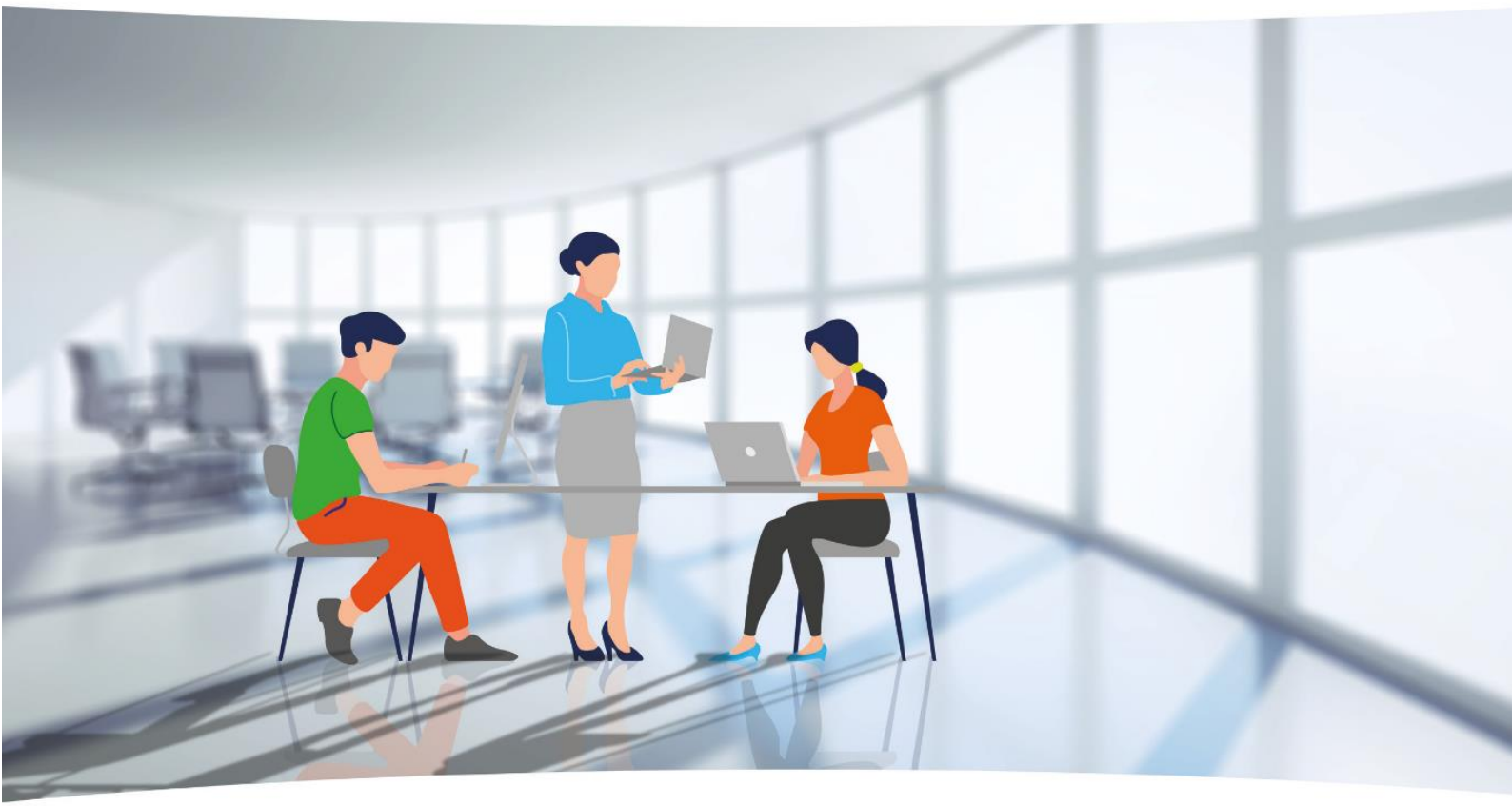
UES UNIR

PROTECTION DES DONNEES A CARACTERE PERSONNEL DE L'UNITÉ ÉCONOMIQUE ET SOCIALE (UES) UNIR



Dont le siège social est situé :
38, RUE FRANÇOIS ARAGO
33700 MÉRIGNAC

www.gestform.com

Composé de :
L'ASSOCIATION UNIR, GESTIONNAIRE DES ENTREPRISES ADAPTÉES
Siret : 334 487 337 00035

GESTFORM 33
(Siège)
38, rue François Arago
33700 MÉRIGNAC
Site de Production
32, rue des Berles
33185 LE HAILLAN

GESTFORM 31
Site de Production
14, rue François Verdier
31830 PLAISANCE DU TOUCH

GESTFORM 92
Site de Production
12, avenue de Verdun 1916
92250 LA GARENNE COLOMBES

Et de :
LA SASU
GESTFORM DÉVELOPPEMENT
Siret : 850 148 933 00011

38, rue François Arago
33700 MÉRIGNAC

I. PRESENTATION DU DOCUMENT

1. INTRODUCTION

La protection des Données à Caractère Personnel (DCP) est une priorité et une condition majeure de confiance des collaborateurs comme des clients, prospects, fournisseurs ou partenaires des entreprises constituant l'UES UNIR, et donc de sa réputation. Elle consiste à respecter les personnes et à protéger les informations les concernant.

Par ailleurs, la législation européenne exige que les données personnelles soient protégées : l'UES UNIR s'engage à respecter ces obligations légales.

2. CONTEXTE REGLEMENTAIRE

La protection des DCP (Données à Caractère Personnel) est une obligation pour l'ensemble des entreprises et sites de l'UES UNIR, qui s'inscrit initialement dans un cadre juridique régi par la directive européenne 95/46/CE du 24 octobre 1995 et en France par la loi Informatique et Libertés du 6 janvier 1978 modifiée.

Elle est fondée sur un principe de transparence visant à respecter la vie privée des personnes concernées conformément à la réglementation en vigueur en France et en Europe dont le cadre a été profondément renouvelé par le Règlement Général sur la Protection des Données (RGPD : règlement UE 2016/679 du Parlement Européen et du Conseil du 27 avril 2016), entré en application le 25 mai 2018. C'est le sens que ce règlement européen vient compléter et renforcer les obligations existantes sur le plan national :

- Il conforte la place de l'individu au cœur du système juridique, technique et éthique de la protection des données à caractère personnel en Europe et lui offre de nouveaux droits ou garanties pour lui permettre de mieux maîtriser le devenir de ses données : meilleure information, extension du consentement, renforcement des droits d'accès, d'opposition, de modification, à l'oubli et création d'un droit à la portabilité pour lui permettre de récupérer ses données sous un format aisément réutilisable et compréhensible ;
- Il place les entreprises traitant des DCP dans une logique de responsabilisation en y incluant les sous-traitants. Chacune à son niveau doit protéger les DCP par la mise en place de mesures physiques, organisationnelles et techniques adaptées aux risques sur la vie privée des personnes concernées, pour les traitements existants ou nouveaux ;
- Il entérine la nécessité de tracer les actions, les mesures de pilotage et de sécurisation des données personnelles (obligation de tenue d'un registre) et encadre les nouvelles pratiques technologiques (profilage, pseudonymisation) ;
- Enfin, il étend le champ des échanges avec les autorités de contrôles (obligation de notification de violation de DCP, consultation préalable pour les traitements susceptibles d'engendrer un risque élevé), renforce le contrôle du régulateur et son pouvoir de sanction (**4% du chiffre d'affaires mondial de l'UES UNIR, ou 20 M€** - le montant le plus élevé étant retenu). Il autorise en outre les actions de groupe en réparation des dommages.

3. OBJECTIFS

La présente Politique a pour objectif de décrire les principes applicables par l'UES UNIR (en particulier pour le respect du Règlement (UE) 2016/679 du Parlement et du Conseil du 27 Avril 2016).

Elle présente les principes généraux et l'organisation mise en place par l'UES UNIR pour assurer la bonne application de cette législation, et rassemble l'ensemble des principes à suivre par et pour ses collaborateurs.

Ce document constitue la politique de protection des DCP de l'UES UNIR lorsque ces données font l'objet d'un traitement, c'est-à-dire de toutes opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de DCP contenues ou appelées à figurer dans un fichier, un outil ou dans une base de données. Le traitement comprend la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Il définit les principes directeurs de la protection des DCP applicables à l'ensemble des entreprises et sites de l'UES UNIR. La politique de protection des DCP s'inscrit dans la stratégie de maîtrise des risques réglementaires et opérationnels de l'UES UNIR.

4. CHAMP D'APPLICATION ET D'EXECUTION

4.1. DONNEES CONCERNEES PAR CETTE POLITIQUE

La présente Politique s'applique au traitement de toutes les données personnelles relatives aux salariés, clients, fournisseurs, ou partenaires commerciaux, réalisés par l'UES UNIR ou les prestataires agissants ou traitant les données personnelles pour le compte de l'UES UNIR.

4.2. PERIMETRE D'APPLICATION JURIDIQUE

La présente Politique de protection des DCP s'applique à compter de sa validation par le Comité de Direction de l'UES UNIR :

- À l'ensemble des salariés des entreprises et sites de l'UES UNIR ;
- Légalement et/ou par le biais de contrats ou annexes, à l'ensemble des sous-traitants de l'UES UNIR ;
- À l'ensemble des partenaires commerciaux de l'UES UNIR ;
- À toutes personnes physiques dont les DCP sont traitées ou collectées au sein de l'UES UNIR : Collaborateurs, dirigeants, Managers, Conseil d'administration, CSE, clients, prospects et prestataires intervenants externes.

Elle est revue au moins sur une base annuelle, ainsi que dans les cas suivants : nouveaux traitements majeurs, événements exceptionnels, changements significatifs ou incidents majeurs.

Toute nouvelle version de ce document est approuvée par le Comité de Direction de l'UES UNIR.

5. ORGANISATION

5.1. ROLES ET RESPONSABILITES

En tant que responsable de traitements général, le président de l'UES UNIR est responsable de la conformité au RGPD pour les entreprises et processus composant l'UES UNIR.

Un DPO a été désigné pour gérer la conformité des deux entreprises composant l'UES UNIR. Il est missionné pour organiser la démarche et est chargé de gérer les révisions du présent document.

5.2. LE DATA PROTECTION OFFICER (DPO)

L'UES UNIR a désigné un Data Protection Officer (DPO), ou Délégué à la Protection des données en français, dont le statut est défini par le RGPD.

Les missions du Data protection Officer sont précisées ci-dessous :

- Informer et conseiller son responsable de traitement – ainsi que l'ensemble de nos personnels - sur les obligations qui leur incombent en vertu du RGPD et d'autres dispositions en matière de protection de données à caractère personnel ;
- Si besoin, informer et conseiller son responsable de traitement des manquements constatés, conseiller dans les mesures à prendre pour y remédier, et soumettre les arbitrages nécessaires;
- Veiller à la mise en œuvre de mesures appropriées pour permettre de démontrer que les traitements mis en œuvre par l'UES UNIR sont effectués conformément au RGPD, et si besoin, réexaminer et actualiser ces mesures ;
- Veiller à la bonne application du principe de protection des données dès la conception et par défaut dans tous nos projets comportant un traitement de données personnelles ;
- Auditer et contrôler, de manière indépendante, le respect du RGPD par les entreprises composant l'UES UNIR, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel en participant aux opérations de traitement et les audits s'y rapportant ;
- Piloter la production et la mise en œuvre de politiques, de lignes directrices, de procédures et de règles de contrôle pour une protection efficace des données personnelles et de la vie privée des personnes concernées ;
- Assurer la bonne gestion des demandes d'exercice de droits, de réclamations et de requêtes formulées par des personnes concernées par nos traitements, et s'assurer de leur transmission aux services intéressés et apporter à ces derniers votre conseil dans la réponse à fournir aux requérants ;

- Être l'interlocuteur privilégié de l'Autorité de contrôle et coopérer avec elle ;
- Dispenser des conseils en ce qui concerne les études d'impact sur la vie privée et en assurer la pertinence ;
- Mettre l'UES UNIR en position de notifier d'éventuelles violations de données auprès de l'Autorité de contrôle et porter conseil au Responsable de traitements, notamment concernant les éventuelles communications aux personnes concernées et les mesures à apporter ;
- Tenir l'inventaire et documenter les traitements de données à caractère personnel des entreprises composant l'UES UNIR en tenant compte du risque associé à chacun d'entre eux compte tenu de sa nature, sa portée, du contexte et de sa finalité ;
- Présenter un bilan annuel des activités au responsable de traitements.

II. PRINCIPES DE PROTECTION DES DONNEES PERSONNELLES

1. LICEITE DU TRAITEMENT

1.1. CONDITIONS DE TRAITEMENT DES DONNEES PERSONNELLES

Les données personnelles ne peuvent être traitées que pour un usage déterminé, explicite et légitime : c'est le principe de finalité.

Conformément à l'article 5 du RGPD :

- Les données collectées sont traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ;
- Elles sont collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement d'une manière incompatible avec ces finalités ; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités) ;
- Elles sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;
- Elles sont exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables sont prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude) ;
- Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);
- Elles sont traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité)

La base légale d'un traitement est ce qui autorise légalement sa mise en œuvre, ce qui donne le droit à un organisme de traiter des données à caractère personnel. On peut également parler de « fondement juridique » ou de « base juridique » du traitement. Ainsi l'UES UNIR peut traiter les données personnelles si le traitement est justifié par l'une des 6 bases légales décrites ci-dessous et **mentionnées à l'article 6 du RGPD** :

- **Le consentement de la personne**

Si la licéité [1]du traitement repose sur cette base légale, l'UES UNIR ne doit traiter les données personnelles qu'avec le consentement de la personne concernée.

- **L'exécution d'un contrat**

Sur cette base légale, la licéité du traitement repose sur une situation pour laquelle le traitement des données personnelles est nécessaire à l'exécution d'un contrat ou l'application de conditions générales de vente.

- **La mission d'intérêt public :**

Le traitement est nécessaire à l'exécution d'une mission d'intérêt public.

- **L'intérêt légitime du responsable de traitement**

L'UES UNIR peut traiter les données personnelles lorsque ses intérêts légitimes le justifient, dans le strict respect des droits et intérêts des personnes dont les données sont traitées.

Parmi les cas d'intérêt légitime du responsable de traitement figure :

- La sécurité, et en particulier les activités de sécurité de l'information, des biens et des réseaux, la journalisation des accès, les tests d'intrusion, audit techniques et recherches de vulnérabilités, collecte de preuves suite à incidents de sécurité,
- Les activités mises en œuvre à des fins de prévention de la fraude,
- Les activités nécessaires aux opérations de prospection commerciale
- Les activités de gestion administrative interne.

- **Le respect d'une ou plusieurs obligations légales**

Cette base s'applique aux cas dans lesquels l'UES UNIR est **légalement tenu** de procéder à un traitement.

On peut en citer pour exemple le respect des réglementations fiscales : L'UES UNIR peut collecter des informations fiscales concernant ses salariés et les transmettre à des tiers obligatoires (URSSAF, retraite, etc…)

- **La sauvegarde des intérêts vitaux**

Il s'agit des cas où le traitement est nécessaire pour protéger les intérêts vitaux d'une personne par exemple, en cas d'urgence médicale.

Lorsqu'un même traitement de données poursuit plusieurs finalités, c'est-à-dire plusieurs objectifs, l'UES UNIR défini une base légale pour chacune de ces finalités. Les bases légales pour une même finalité ne seront jamais cumulées.

[1] Permis par la loi

1.2. CONSENTEMENT

Dans les cas où le traitement repose sur le consentement, les entités de l'UES UNIR s'assurent :

- De pouvoir démontrer que la personne concernée a donné son consentement au traitement de DCP la concernant ;
- Que si le consentement est donné dans le cadre d'une déclaration écrite, la demande de consentement est présentée sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples ;
- Que la personne concernée ait le droit de retirer son consentement à tout moment, elle en est informée avant de donner son consentement ;
- Que ce consentement est géré conformément aux exigences suivantes :
  - Il est aussi simple de retirer que de donner son consentement ;
  - Le consentement est donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des DCP la concernant ;
  - Cela pourrait se faire notamment en cochant une case lors de la consultation d'un site internet, en optant pour certains paramètres techniques pour des services de la société de l'information ou au moyen d'une autre déclaration ou d'un autre comportement indiquant clairement dans ce contexte que la personne concernée accepte le traitement proposé de ses DCP ;
  - Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité ;
  - Le consentement donné doit valoir pour toutes les activités de traitement ayant la ou les mêmes finalités ;
  - Lorsque le traitement a plusieurs finalités, le consentement doit être donné pour l'ensemble d'entre elles ;
  - Si le consentement de la personne concernée est donné à la suite d'une demande introduite par voie électronique, cette demande doit être claire et concise et ne doit pas inutilement perturber l'utilisation du service pour lequel il est accordé.

2. SPECIFICATIONS DE LA FINALITE, LIMITATION ET MINIMISATION DES DONNEES PERSONNELLES

2.1. ENGAGEMENTS DE L'UES UNIR

L'UES UNIR garantit que les données personnelles ne sont traitées que dans la mesure où elles sont adéquates, pertinentes et non excessives à des fins précises, explicites et légitimes.

Pour chaque processus pour lesquels la finalité n'est pas liée à l'exécution d'un contrat, à un intérêt légitime, au respect d'une ou plusieurs obligations légales, ou à la protection des intérêts vitaux d'une personne, l'UES UNIR spécifie les objectifs pour lesquels il va collecter et traiter les données.

L'identification de ces fins doit être faite avant de recueillir des données. Pour les clients et prospects en particulier, une information claire et transparente doit être donnée.

2.2. REGLES POUR GARANTIR LA MINIMISATION DES DONNEES ET LA LIMITATION DES OBJECTIFS

- Les données personnelles doivent être adéquates, pertinentes et limitées à celles qui sont nécessaires au vu des finalités pour lesquelles elles sont collectées et/ou traitées.
- En cas de transfert, de divulgation ou de partage de données personnelles à des tiers, l'UES UNIR doit vérifier si les données personnelles sont strictement nécessaires au traitement réalisé par les tiers, hors organismes sociaux.
- Les données personnelles non nécessaires, non pertinentes, ou qui peuvent devenir non pertinentes avec le temps doivent être supprimées ou anonymisées (Cas des statistiques ou reporting par ex.).

3. EXACTITUDE DES INFORMATIONS ET MISE A JOUR

L'UES UNIR doit prendre toutes les mesures pour s'assurer que les données personnelles qu'il traite soient exactes et le cas échéant, corrigées et tenues à jour.

Les données personnelles qui sont inadaptées ou incomplètes, au regard des finalités pour lesquelles elles ont été collectées ou pour lesquelles elles sont traitées, devront être rectifiées voire effacées.

4. CONSERVATION DES DONNEES PERSONNELLES

4.1. DUREE DE CONSERVATION DES DONNEES ET D'ARCHIVAGE

L'UES UNIR assure que les données personnelles ne seront pas conservées plus longtemps que nécessaire, conformément aux besoins des métiers concernés et aux exigences d'archivage légales (en cas de contentieux par exemple, ou pour obligations fiscales ou légales).

Pour référence, voici les durées de conservation recommandées selon la finalité des traitements les plus courants :

POUR LA GESTION DE L'UES UNIR :

Finalité du traitement	Durée de conservation	Fondement juridique
Constitution et gestion d'un fichier de prospects	3 ans à compter de leur collecte par le responsable de traitement ou du dernier contact émanant du prospect	Norme simplifiée n°48
Envoi de sollicitations (emailings, appels téléphoniques, télécopies, SMS, etc.)	3 ans à compter de leur collecte par le responsable de traitement ou du dernier contact émanant du prospect	Norme simplifiée n°48
Vidéosurveillance	1 mois	Loi 95-73 du 21-01-1995
Gestion des commandes, des livraisons et de la facturation	10 ans	Article L123-22 alinéa 2 du Code de commerce Norme simplifiée n°48
Cookies et traceurs de connexions	13 mois	✓ Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée. ✓ Délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs »
Gestion du personnel	5 ans (en archivage intermédiaire) à compter du départ du salarié	✓ R. 1221-26 du code du travail ✓ Norme simplifiée n°46
Gestion de la paie	5 ans à compter du versement de la paie	✓ Article L3243-4 du Code du travail ✓ D. 3243-8 du code du travail ✓ L. 243-16 du code sécurité sociale ✓ L. 123-22 du code du commerce
Fichiers de recrutement	Destruction immédiate si le candidat n'est pas retenu ni pour le poste à pourvoir ni dans le cadre d'un futur recrutement. Possibilité de conserver le CV pendant 2 ans après le dernier contact avec le candidat	Recommandation 85-44 du 1er octobre 1985. Recommandation n°02-017 du 21 mars 2002
Gestion des réunions des instances représentatives du personnel	Les données relatives aux sujétions particulières ouvrant droit à congés spéciaux ou à un crédit d'heures de délégation ne sont pas conservées au-delà de la période de sujétion de l'employé concerné	Norme simplifiée n°46
Gestion de l'annuaire du personnel	Les données ne sont pas conservées au-delà de la période d'emploi de la personne concernée	Norme simplifiée n°46

Finalité du traitement	Durée de conservation	Fondement juridique
Contrôle de l'utilisation d'internet par les salariés	✓ 1 an ○ 3 mois en base active ○ 9 mois en archivage intermédiaire	✓ Directive européenne : 1 à 2 ans ✓ L'article 6 de la LCEN : 1 an ✓ La loi anti-terrorisme : 1 an ✓ CNIL : 6 mois ✓ PSSI : 1 an
Contrôle de l'utilisation de la messagerie (outils de mesure de la fréquence, de la taille des messages électroniques, outils d'analyse des pièces jointes, etc.)	✓ 1 an ○ 3 mois en base active ○ 9 mois en archivage intermédiaire	✓ Directive européenne : 1 à 2 ans ✓ L'article 6 de la LCEN : 1 an ✓ La loi anti-terrorisme : 1 an ✓ CNIL : 6 mois ✓ PSSI : 1 an
Gestion de la téléphonie (données relatives à l'utilisation des services de téléphonie : numéros appelés, numéros des appels entrants, etc.)	✓ 1 an ○ 3 mois en base active ○ 9 mois en archivage intermédiaire	✓ Directive européenne : 1 à 2 ans ✓ L'article 6 de la LCEN : 1 an ✓ La loi anti-terrorisme : 1 an ✓ CNIL : 6 mois ✓ PSSI : 1 an
Audits organisationnels et techniques, Activités Inforensique (processus et techniques d'investigation permettant de collecter et d'analyser des éléments ayant valeur de preuves en vue d'une procédure judiciaire), collecte et analyse des journaux technique de sécurité, collecte et analyse de trames réseaux.	✓ Durée du traitement	✓ Directive européenne : 1 à 2 ans ✓ L'article 6 de la LCEN : 1 an ✓ La loi anti-terrorisme : 1 an ✓ CNIL : 6 mois ✓ Article 323-1 du code pénal français ✓ PSSI : 1 an
Contrôle des horaires	Les éléments d'identification ne doivent pas être conservés au-delà de 5 ans après le départ du salarié ou de l'agent de l'entreprise ou de l'administration. Les informations relatives aux horaires des employés peuvent être conservées pendant 5 ans La conservation des données relatives aux motifs d'absence est limitée à une durée de 5 ans	Durée de prescription des salaires article L 143-14 Code du travail ; Article L 3245-1 du Code du travail conformément à l'article 2224 du Code civil Prescription des salaires ; Norme simplifiée n° 42 sauf dispositions législatives contraires
Contrôle d'accès physique	Les éléments d'identification ne doivent pas être conservés au-delà du temps pendant lequel la personne est habilitée à pénétrer dans les locaux concernés. Recommandation : 3 mois (historique des passages)	Délibération 97-044 du 10-06-1997 Norme simplifiée n°42 AU- 008 et AU-007
Mandats des représentants du personnel (nature du mandat et syndicat d'appartenance)	6 mois après fin du mandat	✓ Article L 425-1 du Code du travail ✓ Article L 2411-5 du Code du travail ✓ L. 2142-1-3 du code du travail
Géolocalisation des véhicules	1 an	Recommandation CNIL
Statistiques de mesures d'audience (Site WEB)	6 mois	Norme simplifiée n°48
Gestion d'une lettre d'information	Jusqu'à désabonnement de la personne concernée	Article 6-5° de la loi n°78-17 modifiée
Procédure d'habilitation relative à la protection du secret	10 ans par l'officier de sécurité central de l'UES UNIR 1 an après la fin de validité de l'avis de sécurité émis par le service enquêteur	https://www.legifrance.gouv.fr/loda/id/JORFTEXT000024880909/ https://www.cnil.fr/fr/declaration/ru-016-gestion-des-habilitations-secret-defense

POUR LES PRESTATIONS DE SERVICES

Dans le cadre des prestations de services réalisées pour le compte de ses clients, l'UES UNIR est amené à conserver les données traitées pour répondre à un besoin de service après-vente et réclamations.

Prestations de services	Durée de conservation (Par défaut)	Fondement juridique
Pôle Ressources humaines	1 mois	SAV client & gestion des réclamations
Pôle éditique et relation clients	1 mois	SAV client & gestion des réclamations
Pôle services financiers	1 mois	SAV client & gestion des réclamations
Pôle numérisation industrielle	1 mois	SAV client & gestion des réclamations
Pôle Facilities Management	1 mois	SAV client & gestion des réclamations

Dans le cadre de prestation entrainant la numérisation et/ou livraison pour archivage de documents dans un outil de GED ou SAE, les délais de durées de conservation débuteront à partir de la date de livraison des fichiers numérique. La suppression de tous les objets numériques produits aura lieu une fois cette durée atteinte sans possibilité de restauration.

Cette présente politique définit par défaut les durées de conservation applicables sur les prestations de services réalisées en production. L'UES UNIR réalisant ses prestations conformément aux directives de ses clients, toutes exigences différentes à celles déclinées dans cette présente politique devra faire l'objet d'une annexe ou contrat spécifique détaillant celles-ci.

REMARQUES GENERALES

Les données utilisées à des fins statistiques ne sont plus qualifiées de données à caractère personnel dès lors qu'elles auront ont été dûment anonymisées ou pseudonymisées

L'UES UNIR doit par ailleurs prendre des mesures raisonnables pour détruire les données personnelles lorsque :

- Elles ne sont plus requises pour les fins pour lesquelles elles ont été collectées ;
- La période maximale d'archivage permise par la loi applicable (le cas échéant) est écoulée.

4.2. CAS DES DONNEES CLIENTS ET PROSPECTS

L'UES UNIR s'engage à ne pas conserver les données personnelles d'un client ou d'un prospect plus de 3 ans à l'issue de la fin de la relation commerciale avec cette personne. La relation commerciale est marquée par différents points de contact, tels que (liste non exhaustive) :

- Une commande
- Une relance commerciale positive
- Un consentement (Opt-in) du client ou prospect (s'il n'a pas dit "oui", c'est "non")

La durée de conservation de 3 ans démarre à la date du dernier contact avec le client ou le prospect. Ce dernier contact marque la fin de la relation commerciale entre l'UES UNIR et cette personne.

Pour pouvoir justifier de conserver les données personnelles d'un client ou prospect, l'UES UNIR peut engager des actions de communication visant par exemple à faire renouveler l'inscription à la newsletter, à une démarche commerciale.

Si, malgré ces actions, aucun contact avec le client ou prospect n'est survenu dans un délai de 3 ans, l'UES UNIR s'engage à supprimer ses données personnelles et à en faire la demande auprès des tiers à qui les données ont été transférées.

5. CAS DES DONNEES TRAITEES DANS LE CADRE DES PRESTATIONS DE SERVICES

OBLIGATIONS GENERALES

L'UES UNIR s'engage à :

- Traiter les Données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la sous-traitance ;
- Informer préalablement le client en cas de traitement des Données en dehors du territoire français et s'engage à demander l'autorisation écrite préalable du client en cas de traitement des Données en dehors du territoire de l'Union Européenne et de l'Espace Économique Européen (EEE).
- Traiter les Données conformément aux instructions documentées du client.
- Si aucune instruction documentée n'est fournie, l'UES UNIR appliquera cette politique par défaut.
- Garantir la confidentialité des Données traitées dans le cadre du Contrat ;
- Veiller à ce que les personnes autorisées à traiter les Données en vertu du Contrat :
  - S'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
  - Reçoivent la formation nécessaire en matière de protection des données à caractère personnel ;
- Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut.

SOUS-TRAITANCE

L'UES UNIR peut faire appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Le client dispose **d'un délai minimum de 1 mois** à compter de la date de réception de cette information **pour présenter ses objections**. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations

III. DROITS DE LA PERSONNE CONCERNEE

1. DANS LE CADRE DE L'UES UNIR

L'UES UNIR reconnait et respecte les droits des personnes concernées et met en œuvre les moyens nécessaires permettant aux personnes concernées d'exercer les droits mentionnés ci-après.

Les demandes d'exercice des droits sont transmises à tous tiers à qui les données ont été transférées.

L'UES UNIR s'engage à répondre sans frais et dans les meilleurs délais (un mois maximum par défaut, étendu à 2 mois en cas de difficultés techniques particulières) aux demandes légitimes d'exercice des droits suivants :

- **Droit à l'information préalable**

Les entités de l'UES UNIR s'assurent que toute information et communication aux personnes concernées relative au traitement de DCP est aisément accessible, facile à comprendre, et formulée en des termes clairs et simples. Elles s'assurent également que les personnes physiques sont informées, dès la collecte, de l'identité du responsable du traitement, des finalités du traitement, des risques, règles, garanties, droits et modalités d'exercice de ces droits liés au traitement de DCP.

Lorsqu'elles ont l'intention d'effectuer un traitement ultérieur des DCP pour une finalité autre que celle pour laquelle les DCP ont été initialement collectées, les entités de l'UES UNIR fournissent au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente.

- **Droit d'accès**

Les personnes concernées peuvent soumettre une demande d'accès. L'UES UNIR leur fournira une copie de toutes les données qu'il détienne à leur sujet.

- **Droit de rectification**

Si une personne concernée découvre que les informations détenues à son sujet par l'UES UNIR sont inexactes ou incomplètes, il peut demander à ce qu'elles soient mises à jour.

- **Droit d'effacement et droit à l'oubli**

Dans certains cas, les personnes concernées peuvent demander à ce que l'UES UNIR suppriment leurs données. Par exemple lorsque les données ne sont plus nécessaires, lorsque les données sont traitées de manière illégitimes ou lorsqu'elles ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées. Cela comprend les cas où les personnes concernées retirent leur consentement.

- **Droit d'opposition**

Les personnes concernées peuvent s'opposer au traitement des données personnelles collectées.

L'UES UNIR doit arrêter de traiter des informations à moins de pouvoir avoir des raisons légitimes sérieuses au traitement.

- **Droit à la portabilité**

Les entités de l'UES UNIR traitent sans frais les demandes de portabilité des DCP et s'engagent à les fournir à la personne concernée dans un format structuré, couramment utilisé et lisible par machine.

- **Droit à la limitation**

Les entités l'UES UNIR limitent les traitements aux seules finalités pour lesquelles les DCP sont collectées et traitent les demandes légitimes de limitation de traitement de DCP des personnes concernées dans les plus brefs délais.

Le tableau suivant récapitule les exercices des droits à prévoir suivant les bases légales choisies :

	Droit d'accès	Droit de rectification	Droit à l'effacement	Droit à la limitation du traitement	Droit à la portabilité	Droit d'opposition
Consentement	Oui	Oui	Oui	Oui	Oui	Retrait du consentement
Contrat	Oui	Oui	Oui	Oui	Oui	Non
Intérêt légitime	Oui	Oui	Oui	Oui	Non	Oui
Obligation légale	Oui	Oui	Non	Oui	Non	Non
Intérêt public	Oui	Oui	Non	Oui	Non	Oui
Intérêts vitaux	Oui	Oui	Oui	Oui	Non	Non

Il est possible pour une personne concernée de formuler des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès.

Les droits peuvent-être exercés auprès du Délégué à la Protection des Données Personnelles de l'UES UNIR à l'adresse suivante :

GESTFORM

À l'attention de M. le Délégué à la protection des données
38, rue François Arago
33700 MERIGNAC

Par mail à l'adresse : dpo@gestform.com

Avant de répondre à votre demande, L'UES UNIR est susceptible de vérifier l'identité de la personne concernée et/ou lui demander de fournir davantage d'informations. Nous nous efforçons de donner suite aux demandes dans un délai raisonnable et, en tout état de cause, dans les délais fixés par la loi d'1 mois, avec la possibilité de deux mois supplémentaires si la question est complexe.

En cas de réponse insatisfaisante, L'internaute peut introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Il est important que les informations transmises soient exactes.

2. DANS LE CADRE DE LA SOUS-TRAITANCE

Dans la mesure du possible, l'UES UNIR s'engage à aider ses clients à s'acquitter de leur obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

3. TRAÇABILITE DE L'EXECUTION DES DEMANDES DE DROITS

Toutes les demandes de droits des personnes concernées sont tracées dans un registre central maintenu par l'UES UNIR, permettant le suivi des demandes jusqu'à leur exécution.

IV. RESPONSABILITE

1. RESPONSABLES DE TRAITEMENTS

Responsable de traitement (Processus)

Un responsable de traitement est identifié pour chaque traitement mis en œuvre au sein de l'UES UNIR directement ou indirectement, dans tous les processus. Par défaut, ce sont les managers de chaque processus métier.

- Tous les traitements sont déclarés auprès du DPO, au travers d'un formulaire ;
- Une analyse est systématiquement réalisée pour tout nouveau traitement afin de déterminer si l'entité juridique de l'UES UNIR est le « responsable de traitement », « co-responsable du traitement » ou « sous-traitant » ;
- Le responsable du traitement détermine de manière claire et précise les finalités et les moyens de chacun des traitements de DCP qu'il met en œuvre avec l'aide des ressources et compétences internes ;
- Le responsable du traitement définit les moyens de mise en œuvre du traitement, et peut décider de l'arrêt du traitement ;
- Lorsque l'entité juridique de l'UES UNIR est « sous-traitant », elle collecte et traite les DCP dans un cadre strictement conforme à la législation ou aux directives écrites de ses clients.

Les managers étant responsables de leurs traitements, ils sont garant du respect de la présente politique et sont en mesure de démontrer qu'elle est respectée, y compris l'efficacité des mesures physiques, techniques et organisationnelles (principe de responsabilité).

2. REGLES DE PROTECTION POUR LES DONNEES SENSIBLES

Les données dites sensibles sont les informations concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle.

Les données concernant des personnes de moins de 15 (quinze) ans, considérées comme mineurs par la législation française sur la protection des données personnelles, sont également des données dont l'UES UNIR souhaite encadrer le traitement.

2.1. REGLES FONCTIONNELLES

L'UES UNIR s'engage à respecter les règles suivantes :

- Le traitement des données sensibles doit être enregistré dans le registre des activités de traitement ;
- Une étude d'impact relative à la vie privée (EIVP ou PIA) doit être effectuée avant chaque nouveau traitement de données sensibles ;
- En fonction des risques identifiés lors de l'EIVP, des mesures de sécurité supplémentaires pourraient devoir être appliquées à des données sensibles.

2.2. MESURES SPECIFIQUES POUR PROTEGER LES DONNEES SENSIBLES

L'UES UNIR s'engage à assurer la sécurité des données personnelles (Disponibilité, Intégrité, Confidentialité, Traçabilité), en particulier des éventuelles données sensibles manipulées.

Concernant les données de santé, l'UES UNIR limite la collecte de données de santé au processus RH et paie, afin de satisfaire à ses obligations d'entreprise adaptée ayant 55% de personnes en situation de handicap dans ses effectifs.

Concernant les données sur l'appartenance syndicale des collaborateurs, l'UES UNIR s'engage à limiter l'accès à ces informations aux équipes de la Direction des Ressources Humaines contribuant aux traitements pour lesquels ces données sont collectées.

Enfin, concernant les autres données sensibles (informations concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, ou la vie sexuelle), l'UES UNIR préconise de ne pas les collecter ni les manipuler.

3. PROTECTION DES DONNEES DES LA CONCEPTION (PRIVACY BY DESIGN)

Les systèmes et la technologie mis en œuvre et utilisés par l'UES UNIR, dans le cadre de ses activités internes comme de ses services et produits, doivent être conçus de manière à assurer que, par défaut et dès les phases de conception :

- Une analyse des risques ou d'impacts soit réalisée ;
- Le traitement des données personnelles est limité à ce qui est nécessaire ;
- L'accès aux données personnelles est limité aux seules personnes qui doivent y avoir accès ;
- La durée de conservation des données n'excède pas la durée légale ou recommandée pour la finalité du traitement ;
- Les mesures de sécurité nécessaires et suffisantes sont mises en œuvre pour répondre aux risques identifiés et sécuriser l'information et les données à caractère personnel, conformément aux exigences de nos clients, ou par défaut, aux règles définies dans la politique de sécurité des systèmes d'information (PSSI) de l'UES UNIR
- La règlementation en vigueur sur la protection des données personnelles est respectée.
- L'anonymisation systématique des données dans le cadre de développement informatique

Ces obligations s'appliquent à l'utilisation des données personnelles au regard de la finalité de traitement envisagé pour chacune des différentes catégories de données personnelles collectées par l'UES UNIR.

4. ÉTUDE D'IMPACT - METHODOLOGIE EIVP

Les Études d'Impact relatives à la protection de la Vie Privée (EIVP), ou Privacy Impact Assessment (PIA) en anglais, se définissent comme une méthodologie d'analyse d'un projet afin d'identifier l'impact que ce projet pourrait avoir sur la protection des données personnelles, et de préciser des recommandations pour la gestion, la minimisation ou l'élimination de cet impact.

Les EIVP permettent à l'UES UNIR de déterminer les mesures appropriées à prendre afin de démontrer que le traitement est conforme à la législation sur la protection des données personnelles.

Les responsables de traitement s'engagent à effectuer une EIVP lorsque leur traitement des données personnelles peut présenter un risque pour les droits et les libertés des personnes.

Dans le cadre des prestations de services réalisées en production, l'UES UNIR aide ses clients pour la réalisation d'analyses d'impact relative à la protection des Données, dès lors qu'il prend en charge des traitements dont le responsable considère qu'ils justifient de cette démarche.

Le cas échéant, l'UES UNIR aide le client pour la réalisation de la consultation préalable de l'autorité de contrôle

V. SECURITE DES DONNEES PERSONNELLES ET CONFORMITE RGPD

1. MESURES DE SECURITE

Les données personnelles doivent être traitées de manière à permettre un niveau approprié de sécurité, y compris la protection contre le traitement non-autorisé ou illicite, ainsi que la perte, la destruction ou les dommages d'origine accidentelle, et doivent être assurées par :

- **Des mesures physiques :** Sécurité du papier, sécurité des accès physiques, etc. ;
- **Des mesures techniques :** par exemple contrôles techniques, chiffrement, sécurité physique des flux de données, etc. ;
- **Des mesures d'organisation :** par exemple ségrégation des tâches et des responsabilités, des environnements techniques, gestion des incidents, des changements et des failles de sécurité portant sur les données, limitation des accès aux stricts besoins opérationnels, définition des durées de conservation, définition des moyens de contrôle, formation du personnel, etc.
- **Le respect des politiques de sécurité** établies dans le Système de Management de la Sécurité de l'Information (SMSI)

Dans le cadre des prestations de services réalisées en production, en l'absence de recommandations ou exigences de sécurité clients, l'UES UNIR s'engage sur son devoir de conseil et mettra en œuvre par défaut, les mesures physiques, organisationnelles et techniques appropriées aux risques pour garantir un niveau de sécurité adapté.

La non prise en compte par nos clients de mesures recommandées par l'UES UNIR devra être validée par écrit.

Pour cela, une politique de sécurité des systèmes d'information (PSSI) décrit les mesures à appliquer en interne.

2. PROCESSUS DE VIOLATION DES DONNEES

En cas de violation de données à caractère personnel, l'UES UNIR a mis en place, conformément à la réglementation, un processus afin de prévenir les autorités de contrôle compétentes ainsi que les responsables de traitement lorsque l'UES UNIR est sous-traitant.

Tout incident réel ou supposé doit être signalé immédiatement après en avoir pris connaissance, selon la procédure de « Gestion des incidents et de violation de données à caractère personnel ». **L'UES UNIR, représenté par son DPO, doit notifier la CNIL dans un délai maximum de 72h** après qualification de l'incident.

Si l'impact sur les personnes concernées est qualifié d'important, l'UES UNIR s'engage également à notifier ces personnes dans les meilleurs délais (clients, prospects, collaborateurs, instances représentatives du personnel, ou tiers).

Dans le cadre des prestations de services réalisées en production, l'UES UNIR s'engage à **notifier à ses clients, toute violation de Données** dans les meilleurs délais, **au plus tard dans les 24h00**, après en avoir pris connaissance. Cette notification est accompagnée de toute documentation utile afin de permettre au client, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente. Si l'UES UNIR ne peut fournir toutes les informations requises dans les délais car des investigations complémentaires sont nécessaires, la notification se fera en deux temps : une notification initiale comme précédemment indiqué et des notifications complémentaires au fur et à mesure de l'avancée des investigations techniques

3. CONTROLE ET AUDIT DE CONFORMITE RGPD

3.1. POLITIQUE ET PLANS DE CONTROLE DE CONFORMITE

L'UES UNIR a formalisé sa politique de contrôle de conformité RGPD. Cette politique est traduite en plan d'actions, afin de définir les contrôles à mettre en œuvre pour l'UES UNIR, ses sous-traitants et ses partenaires.

Ces programmes d'audits permettent de contrôler périodiquement le respect de la présente Politique et contribuer au respect par l'UES UNIR, par ses salariés et par ses sous-traitants, des lois, règlements et accords contractuels s'appliquant aux données personnelles traitées.

3.2. REPORTING DE CONFORMITE

Le reporting à destination du directeur général est réalisé par le DPO et permet à la Direction de l'UES UNIR de disposer régulièrement d'une vision consolidée des dispositifs de protection des DCP.

3.3. RELATION AVEC LES AUTORITES DE CONTROLE

L'UES UNIR collabore avec l'autorités de contrôle pour toute question relative à la protection des DCP ou bien dans le cadre de leurs procédures d'audit. En France, l'autorité de contrôle est la CNIL.

L'UES UNIR met en place les processus permettant de se conformer et d'appliquer les recommandations de ces autorités conformément au cadre réglementaire et législatif en vigueur.

Le DPO de l'UES UNIR est l'interlocuteur privilégié de la CNIL.

VI. PROTECTION DES DONNEES DES SITES WEB

L'UES gère un site WEB d'entreprise à vocation publicitaire accessible à l'adresse : https://www.gestform.com. Les paragraphes suivants s'appliquent à tous les autres sites WEB publics potentiellement gérés par l'UES UNIR.

1. PROTECTION DE LA VIE PRIVEE

Les sites WEB publics mises en œuvre par l'UES UNIR respecte la vie privée des internautes et se conforment strictement aux lois en vigueur sur la protection de la vie privée et des libertés individuelles. Aucune information personnelle n'est collectée à l'insu des visiteurs.

Un consentement (Opt-in) du visiteur est systématiquement demandé par case à cocher (s'il n'a pas dit "oui", c'est "non")

Aucune information personnelle n'est cédée à des tiers. Les courriels, les adresses électroniques ou autres informations nominatives recueillies par l'intermédiaire de ce site ne font l'objet d'aucune exploitation et ne sont pas stockées sur la plateforme. Elles sont immédiatement transmises aux responsables de traitement et ne sont conservés que pour la durée nécessaire.

2. TRAITEMENTS

Le site public www.gestform.com mis en œuvre par l'UES UNIR recueille des données à caractère personnelles dans le cadre des traitements suivants :

2.1. ABONNEMENT A LA NEWSLETTER

- **Les données collectées sont :**
  - NOM
  - Prénom
  - Email
- Ces données sont accessibles essentiellement au service commercial
- Elles sont conservées sur une durée de 3 ans
- Le consentement peut être retiré à tout moment

2.2. RUBRIQUE RECRUTEMENT

Dans le cadre du recrutement, l'UES UNIR effectue un traitement des candidatures (CV et Lettre de motivation), adressées directement par les postulants au travers d'un formulaire sur le site www.gestform.com, ou provenant de réseaux spécialisés.

Les seuls destinataires des données à caractère personnel collectées pour ce traitement sont les représentants du service ressources humaines de l'UES UNIR.

Dans le cas où une candidature pourrait correspondre ultérieurement à un nouveau poste vacant, **l'UES UNIR conserve les candidatures pendant deux ans**, sauf demande contraire des personnes concernées, délai à l'issue duquel les données sont détruites.

2.3. RUBRIQUE « CONTACT » (CONTACTEZ-NOUS)

- Cette rubrique permet aux internautes, visiteurs du site WEB, de rentrer en contact avec le service commercial de l'UES UNIR
- Les données collectées sont :
  - NOM
  - Email
- Ces données sont accessibles essentiellement au service commercial
- Elles sont conservées sur une durée de 3 ans
- À tout moment le consentement peut être retiré

En outre, le site n'effectue aucun traitement lié au e-commerce ou vente en ligne.

2.4. DONNEES STATISTIQUES : TRAÇABILITE ET PROFILAGE

Lors de leur navigation sur le site, les internautes laissent des traces informatiques. Cet ensemble d'informations est recueilli à l'aide d'un témoin de connexion appelé cookie qui ne contient, toutefois, aucune information personnelle.

Les outils de mesures d'audience sont utilisés pour obtenir des informations sur la navigation des internautes sur son site. Ils permettent notamment de comprendre comment les utilisateurs arrivent sur un site web ou une application mobile et de reconstituer leur parcours. Utilisant des cookies ou d'autres traceurs, ils peuvent être exemptés de consentement sous certaines conditions.

Conformément à l'article 82 de la loi Informatique et Libertés, le consentement n'est pas requis car le traitement :

- A pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;
- Est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.
- Ne permet pas le suivi global de la navigation de la personne utilisant différentes applications ou naviguant sur différents sites web ;
- Sert uniquement à produire des données statistiques anonymes ;
- Ne conduit pas à un recoupement des données avec d'autres traitements.

Les données collectées ne sont jamais transmises à des tiers.

Dans le but d'améliorer l'ergonomie, la navigation au sein du site, le contenu éditorial et le service aux internautes, l'outil gestionnaire des statistiques du site www.gestform.com stocke des informations relatives au profil des internautes : équipement, navigateur utilisé, origine géographique des requêtes, date et heure de la connexion, navigation sur le site, fréquence des visites, etc. Ces données de connexion permettent des extractions statistiques et sont **conservées pendant 13 mois.**

3. COOKIES

Conformément à la délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée, Et à la délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs.

- La simple poursuite de la navigation sur un site n'est pas considérée comme une expression valide du consentement de l'internaute ;
- Les personnes consentent au dépôt de cookies par un acte positif clair (comme le fait de cliquer sur « j'accepte » dans une bannière cookie). Si elles ne le font pas, aucun cookie non essentiel au fonctionnement du service ne sera déposé sur leur appareil.
- Les utilisateurs sont en mesure de retirer leur consentement, facilement, et à tout moment. Refuser les traceurs est donc aussi aisé que de les accepter.
- Les personnes sont clairement informées des finalités des cookies avant de consentir, ainsi que des conséquences qui s'attachent à une acceptation ou un refus de cookie ;
- Elles sont également informées de l'identité de tous les acteurs utilisant des traceurs soumis au consentement.
- L'UES UNIR est en mesure de fournir, à tout moment, la preuve du recueil valable du consentement libre, éclairé, spécifique et univoque de l'utilisateur
- L'interface de recueil du consentement comprend un bouton « tout accepter » mais aussi un bouton « tout refuser ».
- L'UES UNIR conserve **pendant 6 mois** le consentement aux cookies, et également le refus des internautes, afin de ne pas réinterroger l'internaute à chacune de ses visites.
- En outre, pour que l'utilisateur soit bien conscient de la portée de son consentement, lorsque des cookies permettent un suivi sur des sites autres que le site visité, le consentement est recueilli sur chacun des sites concernés par ce suivi de navigation.

VII. TRANSFERT DES DONNEES PERSONNELLES

1. TRANSFERTS DE DONNEES PERSONNELLES

Tout transfert de données personnelles doit être fondé sur une finalité spécifique et légitime, ne pas violer la loi et être limité au strict nécessaire.

Les transferts de données personnelles doivent figurer dans les registres de traitements de l'UES UNIR.

2. TRANSFERTS DE DONNEES PERSONNELLES A DES SOUS-TRAITANTS

Le sous-traitant est la personne morale qui traite les données personnelles pour le compte du responsable de traitement. Il peut voir sa responsabilité engagée au titre de clauses contractuelles.

L'UES UNIR doit conclure des contrats appropriés avec les prestataires pour s'assurer qu'ils traitent les données personnelles conformément à la réglementation sur la protection des données personnelles, et conformément à la présente Politique. Ces engagements contractuels comprennent notamment :

- La définition, l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel, les catégories de personnes concernées, la description des mesures de sécurité mises en place, et les obligations et les droits ;
- La fourniture des analyses de risques sur la vie privée (EIVP ou PIA), pour les traitements les plus sensibles ;
- L'engagement du sous-traitant à ne pas recruter un autre sous-traitant sans l'autorisation écrite préalable de l'entité concernée l'UES UNIR ;
- L'engagement du sous-traitant de s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits dans le respect du délai légal ;
- L'engagement du sous-traitant à supprimer toutes les DCP ou les renvoyer au responsable du traitement au terme de la prestation de services relatifs au traitement, et de détruire les copies existantes ;
- L'engagement du sous-traitant à notifier à l'UES UNIR, dès que possible, toute violation de DCP le concernant ;
- La possibilité pour l'UES UNIR de réaliser des contrôles, audits ou inspections des dispositifs de protection des DCP ;
- L'engagement du sous-traitant à ne réaliser de traitement transfrontalier qu'après accord préalable de l'UES UNIR et uniquement au sein de l'Union Européenne ou avec un pays présentant un niveau de protection adéquat ;
- L'engagement du sous-traitant à prévenir l'UES UNIR de tout changement significatif dans la gestion des DCP.
- L'UES UNIR s'engage à répercuter les exigences de ses responsables de traitements à ses sous-traitants s'il y fait appel.
- L'UES UNIR se réserve le droit de réaliser des audits auprès des sous-traitants pour s'assurer du respect de leurs engagements. Si l'UES UNIR conclut qu'un sous-traitant ne respecte pas ces obligations, il prendra les mesures appropriées sans délai.

3. TRANSFERTS INTERNATIONAUX

Avant de transférer des données personnelles hors du pays d'origine, l'UES UNIR doit s'assurer que les destinataires ont adopté des garanties appropriées de protection et de sécurité, conformément à la législation sur la protection des données personnelles applicable.

L'UES UNIR ne doit pas transférer des données personnelles à des prestataires extérieurs à l'Espace Économique Européen (EEE), à moins que, par exemple, les clauses contractuelles standard de l'UE approuvées par la Commission européenne ne soient signées par le prestataire si ce dernier est situé dans un pays ne prévoyant pas un niveau adéquat de protection des données personnelles.

VIII. VALIDATION ET MISE EN APPLICATION DE LA POLITIQUE

Pour l'UES,
Monsieur Olivier THERON
Président de l'association UNIR et
Pour la SASU GESTFORM Développement,
Représentant permanent légal de la Présidence, l'Association UNIR

Signé électroniquement par
Olivier THERON
Le 11/06/2024 à 07:53

IX. ANNEXES

GLOSSAIRE

Terme	Définition
Anonymisation	L'anonymisation rend impossible l'identification d'une personne à partir d'un jeu de données et permet, ainsi, de respecter sa vie privée.
Autorité de protection des données	Autorité administrative d'un État membre de l'Union Européenne ou d'un pays dans le monde, ayant notamment vocation à surveiller sur son territoire, le respect des dispositions législatives et réglementaires applicables à la protection des données à caractère personnel. En France, c'est la CNIL
Consentement	Toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des DCP la concernant fassent l'objet d'un traitement.
Délégué à la protection des données à caractère personnel (DPO)	La personne en charge du pilotage des actions mises en œuvre pour le respect de la présente Politique de l'UES UNIR, et de la conformité avec la règlementation en vigueur sur la protection des DCP de manière générale.
Donnée à caractère personnel (DCP)	Toute information se rapportant à une personne physique identifiée ou identifiable (est réputée identifiable une personne qui peut être identifiée) directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.
Catégorie particulière d'une donnée à caractère personnel dite « sensible »	Toute donnée à caractère personnel qui fait apparaître, directement ou indirectement, l'origine raciale ou ethnique, les opinions politiques ou philosophiques, les croyances religieuses, l'appartenance syndicale, ainsi que les données relatives à la santé, les préférences sexuelles ou les données judiciaires d'un individu
Espace Économique Européen	L'ensemble des États membres de l'Union européenne et les membres de l'EEE. Liste consultable : http://accueil-etrangers.gouv.fr/modeles/articles-lies/article/consultez-la-liste-des-pays-de-l
Exportateur de données	Tout responsable de traitement situé dans l'Espace Économique Européen qui transfère directement ou pour le compte duquel l'UES UNIR fait transférer des données à caractère personnel à un Importateur de données dans un pays tiers
Importateur de données	Toute société de l'UES UNIR dans un pays tiers qui reçoit des données à caractère personnel en provenance de l'Espace Économique Européen en vue de leur traitement ultérieur
Pays adéquat	Désigne tout pays faisant partie de l'EEE ainsi que la Principauté d'Andorre, la Suisse, les Îles Féroé, Guernesey, l'Île de Man et Jersey
Pays tiers	Tout État non membre de l'Espace Économique Européen et/ou nécessitant une autorisation de la CNIL préalablement au transfert de Données à caractère personnel conformément à la cartographie suivante : https://www.cnil.fr/fr/la-protection-des-donnees-dans-lemonde
Personne concernée	Toute personne physique dont les données à caractère personnel font l'objet d'un traitement en sa qualité de collaborateur, candidat, Personnel d'une société tierce intervenant au profit de l'UES UNIR, client, prospect ou fournisseur
Profilage	Toute forme de traitement automatisé de DCP consistant à utiliser ces DCP pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique
Pseudonymisation	Le traitement de DCP de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les DCP ne sont pas attribuées à une personne physique identifiée ou identifiable
Responsable de traitement	Toute personne physique ou morale qui détermine les finalités et les moyens du traitement de données à caractère personnel
Sous-traitant	La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable de traitement
Tiers	Toute personne physique ou entité juridique, autorité publique ou tout organisme autre que la personne concernée, le responsable du traitement,

	le prestataire et les personnes ou départements qui, placés sous l'autorité directe du responsable du traitement ou du prestataire, sont chargés de la mise en œuvre du traitement
Traitement	Toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction
Transfert	Toute opération ou ensemble d'opérations permettant de communiquer, copier ou déplacer des données à caractère personnel en utilisant un réseau ou tout autre support, dans la mesure où ces données sont destinées à être traitées par l'Importateur de données
Violation de données à caractère personnel	Toute violation de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données