



## NOS ENGAGEMENTS EN MATIERE DE PROTECTION DES DONNES (RGPD)

D'après notre analyse du rôle et des responsabilités de chaque partie, nous considérons que RESSIF GIE détermine de manière autonome les objectifs et les moyens relatifs au traitement des données à caractère personnelles, et que RESSIF GIE assurera par conséquent la fonction de responsable du traitement des données au sens du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 sur la protection des personnes physiques à l'égard du traitement des données personnelles et sur le libre mouvement de ces données.

En tout état de cause, en notre qualité de service social en entreprise, nous prêtons une attention toute particulière à la protection des données personnelles.

Dans ce cadre, RESSIF GIE s'inscrit dans une démarche globale de mise en conformité avec le Règlement Général sur la Protection des Données :

- Nous avons désigné auprès de la CNIL notre Data Protection Officer
- Nous mettons à jour notre registre des activités de collecte et de traitement de données
- Nous recensons et cartographions nos processus de collecte de données personnelles
- Nous mettons à jour nos contrats avec nos sous-traitants
- Nous continuons à renforcer nos procédures internes afin de garantir au maximum la protection et la sécurité des données.



# POLITIQUE RGPD : TRAITEMENTS DES DONNES

## 1. TRAITEMENT DES DONNES PERSONNELLES

1.1. RESSIF GIE s'engage à traiter les Données Personnelles uniquement pour les besoins de l'exécution des prestations de service social au profit des ses entreprises et structures clientes.

1.2. RESSIF GIE n'a accès qu'aux données personnelles transmises par les collaborateurs qui sollicitent une intervention.

La nature des données transmises dépend de la demande de chaque collaborateur.

Ces données sont en rapport avec la problématique personnelle au sujet de laquelle le salarié sollicitera l'aide d'une assistante sociale. Il peut s'agir notamment de données concernant la santé, la famille, les finances, le logement, la carrière et la situation professionnelle...

1.3. En conséquence, RESSIF GIE s'interdit d'exploiter, pour son propre compte ou pour celui d'un tiers, directement ou indirectement, les Données Personnelles, céder et/ou mettre à disposition de tiers les Données Personnelles à quelles que fins que ce soit et notamment à des fins de prospection commerciale, effectuer des copies de tous

documents et supports d'information contenant des Données Personnelles, à l'exception de celles nécessaires pour les besoins de l'exécution de ses contrats.

1.4. RESSIF GIE s'engage à aider ses clients, à leur demande, pour garantir le respect des obligations prévues aux articles 32 et 36 du RGPD concernant les traitements qu'il effectue, incluant la participation aux éventuelles analyses d'impact et aux mesures d'atténuation des risques susceptibles d'en découler, et, le cas échéant, la participation aux enquêtes ou inspections émanant de l'autorité de contrôle.

1.5. Dans le cas où RESSIF GIE serait chargé de la collecte des Données Personnelles pour le compte d'un Client, celui-ci s'engage, au moment de la collecte des Données Personnelles, à fournir aux personnes concernées par les opérations de traitement, l'information relative aux traitements de données réalisées, conformément aux exigences du RGPD. Les mentions d'information communiquées aux personnes devront être validées préalablement par écrit par le Client concerné.

## 2. CONFIDENTIALITÉ ET SÉCURITÉ DES DONNÉES PERSONNELLES

2.1. RESSIF GIE s'engage à garantir la confidentialité des Données Personnelles.

A ce titre, l'accès aux Données Personnelles est strictement limité aux personnes autorisées en ayant besoin pour la réalisation de l'exécution des contrats qui :

- Signent un contrat écrit dans lequel elles s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité et
- Reçoivent la formation nécessaire en matière de protection des données à caractère personnel

2.2. RESSIF GIE confie l'hébergement des Données Personnelles à un prestataire extérieur (Sté TIMSOFT à Paris) selon les modalités suivantes :

- Mise à disposition de serveurs d'hébergement en environnement HDS (Hébergement Données de Santé) par le Datacentre d'OVH de Roubaix, OVH assurant le bon fonctionnement de la partie matérielle, TimSoft gérant la partie système et applicative
- Architecture de type Cloud Privé

2.3. Les sauvegardes sont assurées au moyen de plusieurs solutions.

- Veeam Backup & Replication

Ce logiciel permet la sauvegarde d'une machine virtuelle à chaud dans son intégralité.

Il est installé au sein d'une machine virtuelle qui lui est propre dans l'environnement et fonctionne sous Windows (Server 2016).

Une fois effectuées, les sauvegardes sont ensuite répliquées sur un deuxième serveur de sauvegarde, mutualisé par TimSoft, hors de l'environnement décrit ci-dessus.

- BackupPC

Ce logiciel est open source et est hébergé sur un serveur de sauvegarde TimSoft mutualisé, bénéficiant de 5 disques de 6 To chacun. Ces disques sont montés en RAID logiciel.

Il permet la sauvegarde des fichiers de l'application ainsi que des bases de données.



### 3. SUIVI DES MESURES DE SÉCURITÉ ET TRAÇABILITÉ

3.1. RESSIF GIE assure un suivi des traces de connexion aux Données Personnelles par les personnels autorisés.

### 4. SORT DES DONNÉES PERSONNELLES

4.1. Les Données Personnelles sont automatiquement et systématiquement détruites à l'issue d'une période de 3 ans, jour pour jour, courant à compter de la date de l'enregistrement de la dernière action effectuée.

4.2. RESSIF GIE s'engage à restituer la totalité des Données

Personnelles exclusivement à la personne concernée et sur sa demande expresse, à l'exclusion de tout autre tiers.

4.3. RESSIF GIE s'engage à ne conserver aucune copie en cas de restitution du dossier à la personne concernée.

## POLITIQUE RGPD : SECURISATION DU SI

### HEBERGEMENT DE L'APPLICATION RESSIFNET EN ENVIRONNEMENT HDS

#### Sécurité de l'accès physique aux serveurs

Accès intérieur : salles restreintes par badge RFID nominatif en fonction des habilitations de chacun, système de vidéosurveillance

Accès extérieur au datacentre: clôtures équipées de barbelés, système de vidéosurveillance et de détection de mouvement

#### Sécurité de l'accès logique aux serveurs et aux applications

Tout le trafic est filtré par un pare-feu, en entrée du serveur

Ports de communication limités au strict nécessaire

Machines virtuelles non accessibles de l'extérieur

L'accès d'administration est protégé par mot de passe et s'effectue via un VPN dont les certificats sont nominatifs et révocables

#### Sécurité du réseau informatique interne

Administration et autorisation par identifiant et mots de passe

Sauvegarde locale et externalisée journalière par incrémentation

Encryptage des données

#### Sécurité des échanges externes

Tous les échanges sont sécurisés en HTTPS via certificat SSL.

#### Chiffrement/Pseudonymisation des données

Anonymisation des données des plateformes de pré-production et de développement

#### Gestion des vulnérabilités et gestion des sauvegardes

Sauvegarde quotidienne des machines virtuelles complètes, des bases de données, des fichiers

Conservation des sauvegardes pendant 7 jours

Sauvegardes répliquées sur un serveur géographiquement distant via un VPN sécurisé

#### Gestion des habilitations

Les habilitations sont gérées par module et/ou par fonctionnalité de l'application. Elles sont attribuées à partir de l'interface administrateur utilisateur par utilisateur

#### Authentification des utilisateurs

Règles de complexité des mots de passe: 8 caractères minimum, 2 types de caractères, 1 chiffre

Vérification des mots de passes : chiffrés via algorithme SHA256 avec grain de sel

Mots de passe sont stockés chiffrés / non réversibles en base de données

Seul l'utilisateur a connaissance de son mot de passe. Au besoin, il peut le modifier à la demande, par une interface d'initialisation / MAJ du mot de passe

Temporisation sur échec d'authentification



## ENGAGEMENT RGPD

### HEBERGEMENT DE L'APPLICATION RESSIFNET EN ENVIRONNEMENT HDS

Les données à caractère personnel collectées font l'objet d'un traitement dont le responsable est RESSIF GIE.

Ces données sont collectées et traitées uniquement dans le cadre de l'exécution du contrat. Elles sont nécessaires à la mise en œuvre de l'accompagnement social des bénéficiaires intérimaires.

Les données personnelles seront conservées dans une base active au titre de la mise en œuvre de l'accompagnement pour une durée de 5 années à compter de la dernière action de prise en charge.

Conformément à la réglementation applicable en matière de données à caractère personnel, la personne concernée dispose d'un droit d'accès, de rectification, d'opposition, de limitation du traitement, d'effacement et de portabilité des données qu'elle peut exercer par mail à l'adresse [dpo@ressif.com](mailto:dpo@ressif.com) ou par courrier à l'adresse suivante RESSIF GIE, A l'attention du Délégué à la protection des données, 1 cours Albert Thomas, 69003 LYON en précisant son nom, prénom, adresse et en joignant une copie recto-verso de sa pièce d'identité.

En cas de difficulté en lien avec la gestion de ses données personnelles, la personne concernée peut adresser une réclamation auprès du délégué à la protection des données personnelles (cf coordonnées ci-dessus) ou auprès de la CNIL.

En outre, le règlement européen 2016/676 UE (RGPD) consacre une logique de responsabilisation de tous les acteurs impliqués dans le traitement de données personnelles, dès lors qu'elles concernent des résidents européens, que ces acteurs soient ou non établis au sein de l'UE.

En cas de difficulté en lien avec la gestion de ses données personnelles, la personne concernée peut adresser une réclamation auprès du délégué à la protection des données personnelles (cf coordonnées ci-dessus) ou auprès de la CNIL.

En outre, le règlement européen 2016/676 UE (RGPD) consacre une logique de responsabilisation de tous les acteurs impliqués dans le traitement de données personnelles, dès lors qu'elles concernent des résidents européens, que ces acteurs soient ou non établis au sein de l'UE.

Dans le cadre des Services proposées par RESSIF GIE, ce dernier est qualifié de responsable de traitement en vertu du Règlement européen n°2016/679 du 27 avril 2016 et de la Loi n°78-17 informatique et libertés du 6 janvier 1978 modifiée. En conséquence, le EDF et RESSIF GIE doivent être considérés comme deux responsables de traitement distincts.

A ce titre, RESSIF GIE s'engage à respecter l'ensemble des obligations mises à sa charge en mettant en place des mesures techniques et organisationnelles permettant d'assurer la sécurité et la confidentialité des données personnelles. Le EDF et RESSIF GIE se prêtent également assistance mutuelle en cas d'inspection, d'audit ou de tout autre requête émanant d'une autorité de protection des données.

Notamment, RESSIF GIE s'engage à s'assurer que toutes les données à caractère personnel aient été et soient collectées et traitées conformément à la réglementation applicable en matière de protection des données. RESSIF GIE prend toutes les mesures nécessaires pour transmettre les notes d'information appropriées aux personnes concernées et garantir la légitimité du traitement des données à caractère personnel. Tout transfert éventuel de données à caractère personnel en dehors de l'espace économique européen, nécessaire à l'exécution du contrat liant le EDF et RESSIF GIE, n'aura lieu qu'après la mise en place des garanties prescrites par les lois applicables en matière de protection des données.

RESSIF s'engage à notifier toute violation de données personnelles à la CNIL, au EDF et le cas échéant aux personnes concernées selon le niveau de risque identifié.