RGPD / FICHE SIGNALETIQUE

Mesures de sécurité organisationnelles et techniques

(DCP = Données à Caractère Personnel)

Exigence ou mesure	Description
Existence du registre des traitements	Oui
Traitements réalisés	Exécution de la ou des mission(s) confiées par le client Exécution des obligations légales, réglementaires et professionnelles Exploitation statistique et de suivi des dossiers en interne
En qualité de	Responsable conjoint de traitement
Base légale	Exécution des obligations contractuelles prévues dans la lettre de mission et ses avenants Exécution des obligations légales, notamment en matière de comptabilité, fiscalité, droit du travail, droit des sociétés
Catégories de DCP traitées	▪ Données d'état civil ▪ Coordonnées ▪ Données concernant la vie personnelle ▪ Données professionnelles ▪ Données bancaires ▪ Données économiques et financières ▪ Données particulières pour la mission Social : NIR, statut de délégué syndical, statut de travailleur handicapé, données concernant la santé
Durée de conservation	Délai légal de conservation
Localisation des données	France, région Pays de la Loire ou Isère
Localisation des personnels agissant sur les DCP	France, régions Pays de la Loire et Bretagne ou Isère
Sous-traitants ultérieurs	▪ Échanges de données informatisés : jedeclare.com ; net-entreprises.fr ▪ Signature électronique : jesignexpert.com ▪ Mission Social : Silaexpert ▪ Mission Juridique : Lexis Nexis
Existence d'un DPO	Non

RGPD / FICHE SIGNALETIQUE

Existence d'un référent RGPD	Oui
Engagement contractuel sur le respect du RGPD en tant que responsable conjoint de traitement	Oui, cf conditions générales annexées à la lettre de mission
Contrôle d'accès physique	▪ Personnel d'accueil présent en permanence à l'entrée principale aux horaires d'ouverture ▪ Ouverture de l'entrée du personnel par badge sur le site principal ▪ Locaux sous alarme en dehors des horaires d'ouverture
Contrôle d'accès logique	▪ Identification et authentification des utilisateurs par mot de passe pour l'accès au poste informatique, au VPN du cabinet et au bureau à distance ▪ Identification et authentification des utilisateurs par mot de passe ou SSO pour la connexion aux logiciels ▪ Antivirus, pare-feu, DMZ
Gestion des comptes à privilèges	▪ Limitation des rôles de confiance
Chiffrement des DCP	▪ Intégralité des sauvegardes cryptées
Protection des infrastructures informatiques	▪ Local serveur fermé à clé en permanence
Journalisation	Non
Sauvegarde des données	▪ Plan de continuité d'activité avec réplication des données sur site de secours ▪ Sauvegardes quotidiennes cryptées ▪ Sauvegardes mensuelles cryptées stockées en dehors des locaux
Anonymisation des DCP	Non, les finalités des traitements rendent impossible l'anonymisation
Contrôle des sous-traitants	▪ Attestation de conformité au RGPD ▪ Fiche descriptive des mesures de sécurité mises en place
Processus de réponse aux droits des personnes concernées	Oui
Processus de notification au responsable conjoint de traitement en cas de violation de DCP	Oui