



## ***Respect de la politique RGPD***

- Nature du contrat : « Accompagnement : formation- bilan de compétences – consulting coaching - supervision »
- Date : durant toute la durée de l'exécution du contrat
- Nom du Prestataire : IZEAS
- Objet : traitement des données à caractères personnels

| <b>Responsable DPO délégué à la protection des données</b>  |
|---|
| Sonia RODRIGUES (déclarée CNIL)   |
| <b>IZEAS a désigné un DPO, conformément à l'article 37 du règlement européen sur la protection des données.<br/>Délégué à la Protection des Données :</b> |
| NOM : Sonia RODRIGUES   |
| Adresse : 44 Route de la Thibaudière – Terves – 79300 BRESSUIRE   |
| Courriel : sonia.rodrigues@izes-formation.fr  |

Dans le cadre de chaque contrat, IZEAS a conscience de devoir gérer le(s) Traitement(s) suivant(s) :

| <b>Traitement</b> | <b>Finalités</b> | <b>Types de données personnelles visées</b> | <b>Personnes concernées</b> |
|-------------------|------------------|---|-----------------------------|
|-------------------|------------------|---|-----------------------------|

A ce titre, IZEAS met en place un Registre des données et des mesures de protection.

### **a) Mesures pour sécuriser le traitement des données personnelles**

**En vue de sécuriser le(s) traitement(s) des données personnelles dans le cadre de l'exécution de ce Contrat, IZEAS met en œuvre les mesures suivantes :**

- ✓ IZEAS, se base sur les recommandations de la CNIL, pour assurer "un niveau de sécurité adapté au risque"

MAJ : 01/07/2024

Auteur : IZEAS



- ✓ **IZEAS a donc mis en place, dans une démarche proactive, une politique de traitement et des mesures techniques et organisationnelles** garantissant ce niveau de sécurité adapté au risque en matière de protection des données personnelles du personnel, des apprenants, des coachés, des clients, des fournisseurs, des intervenants et des partenaires extérieurs.
  
- ✓ IZEAS s'appuie notamment **pour la mise en place de ses procédures de protection, des guides PIA**, pour déterminer les mesures proportionnées aux risques identifiés, en agissant sur :
  - Les « **éléments à protéger** » :  
Minimiser les données, chiffrer, anonymiser, permettre l'exercice des droits, etc.
  - Les « **impacts potentiels** » :  
Sauvegarder les données, tracer l'activité, gérer les violations de données etc.
  - Les « **sources de risques** » :  
Contrôler les accès, gérer les tiers, lutter contre les codes malveillants etc.
  - Les « **supports** » :  
Réduire les vulnérabilités des matériels, logiciels, réseaux, documents papier etc.

Politique :

- ✓ **Désignation d'un Délégué à la Protection des données, déclaré au CNIL**, chargé de s'assurer de la mise en conformité au règlement européen.  
Il est principalement chargé : d'informer et de conseiller le responsable de traitement ou le sous-traitant ainsi que leurs employés, de contrôler le respect du règlement et du droit national en matière de protection des données, de conseiller l'organisme sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution, de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.
  
- ✓ Mise en place de la **tenue d'un registre des traitements (qui documente les données traitées, les finalités, les mesures de sécurité...)**
  
- ✓ **Création d'un lieu de stockage de données sécurisé**
  
- ✓ **Moyen permettant de rétablir la disponibilité des données** à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique
  
- ✓ **Identification régulière des actions à mener pour continuer de se conformer aux obligations actuelles** et à venir (par la formation, et la veille informationnelle), et **identifications claires des traitements à risque** / à caractère sensible
  
- ✓ **Conscience et prise en compte de l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement de données personnelles** (par exemple : faille de sécurité, cyberattaque, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire, etc.)

MAJ : 01/07/2024

Auteur : IZEAS



- ✓ **Mise en place d'un protocole de gestion des réclamations et des demandes des personnes concernées quant à l'exercice de leurs droits** (droits d'accès, de rectification, d'opposition, droit à la portabilité, retrait du consentement) en définissant les acteurs et les modalités (l'exercice des droits de fait notamment par voie électronique)
  
- ✓ Les mesures organisationnelles et techniques sont **réexaminées et actualisées** si nécessaire, et au moins 2 fois par an.
  
- ✓ Le cycle du traitement est le suivant :
  - **Collecte** des données.
  - **Stockage** des données.
  - **Traitement** des données.
  - **Analyse** des données.
  - **Sauvegarde** des données régulière.
  - **Réutilisation** des données.
  - **Suppression** des données
  
- ✓ Exemples d'actions et de mesures en faveur de la protection des données :
  - **Nommer un DPO (CNIL)**
  - **Tenir à jour le registre**
  - **Sensibiliser les utilisateurs**
  - **Sensibiliser et former les sous-traitants (intégration des clauses de protection des données dans les contrats de sous traitance avec les partenaires, assurant leur conformité au RGPD)**
  - **Authentifier les utilisateurs**
  - **Gérer les habilitations**
  - **Gérer les incidents**
  - **Sécuriser les postes de travail (antivirus, pare-feu)**
  - **Sécuriser l'informatique mobile**
  - **Protéger le réseau informatique interne**
  - **Sécuriser les serveurs**
  - **Sécuriser les sites web**
  - **Sauvegarder régulièrement (avec plan de restauration)**
  - **Archiver de manière sécurisée**
  - **Encadrer la destruction des données**
  
- ✓ **Evaluer l'impact (pour identifier et atténuer les risques potentiels)**

## **b) Respect du droit des personnes concernées**

- ✓ IZEAS communiquera aux personnes concernées par les opérations de **traitement leur droit**.
  
- ✓ Ce droit est décomposé comme suit :
  - Droit **d'accès** aux données ;
  - Droit de **rectification** des données ;
  - Droit de **suppression** des données ;



- Droit **d'opposition** au traitement des données ;
- 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)
- Droit de se voir notifier toute **rectification, effacement** de données ou **limitation** du traitement ainsi que le **droit d'être informé sur les destinataires** des données les concernant.

### c) Notification des violations de données à caractère personnel

- ✓ **Mise en place d'un protocole d'urgence : Envoi de notification à l'autorité de protection des données dans les 72 heures**, en cas de violation des données
- ✓ En cas de violation de données à caractère personnel, IZEAS s'engage à **notifier par lettre recommandée avec accusé de réception, sous 48 heures, aux personnes concernées** :
  - La description de la nature de la violation de données à caractère personnel avec une copie des éléments liés à l'incident) y compris, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
  - Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
  - La description des conséquences probables de la violation de données à caractère personnel ;
  - La description des mesures prises ou que le Responsable du Traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.