



# I-VAE

## Guide juridique en matière de sécurisation des données

### Présentation

|                                                                                        |          |
|----------------------------------------------------------------------------------------|----------|
| <b>I- La déclaration à la CNIL .....</b>                                               | <b>3</b> |
| 1.1 La déclaration d'I-VAE à la CNIL .....                                             | 3        |
| 1.2 La mention relative au droit d'accès sur les formulaires papiers .....             | 3        |
| <b>II- La loi informatique et libertés .....</b>                                       | <b>4</b> |
| 2.1 La sécurisation du fichier .....                                                   | 4        |
| 2.2 La confidentialité des données .....                                               | 4        |
| 2.3 La durée de conservation des informations .....                                    | 4        |
| 2.4 L'information des personnes .....                                                  | 4        |
| 2.5 La déclaration du fichier à la CNIL .....                                          | 4        |
| 2.6 La finalité du traitement .....                                                    | 4        |
| <b>III- Les préconisations en matière de sécurité des systèmes d'information .....</b> | <b>5</b> |
| 3.1 La sécurisation du poste .....                                                     | 5        |
| 3.2 Le choix d'un mot de passe fort .....                                              | 5        |
| 3.3 La confidentialité .....                                                           | 5        |
| <b>IV- Pour plus d'informations .....</b>                                              | <b>5</b> |

L'application I-VAE est une plate-forme web sécurisée permettant la gestion et le suivi de parcours de candidats à une VAE avec une remontée statistique ministérielle. Mise en place par l'académie de Strasbourg, cette application est proposée à l'ensemble des DAVA des académies de France.

I-VAE est un outil informatique comportant des données à caractère personnel. De ce fait, l'académie de Strasbourg porte une attention particulière à ce que **les responsables et les personnels des DAVA, utilisateurs de l'application, s'engagent à respecter les dispositions exposées ci-dessous.**

## I- La déclaration à la CNIL

Conformément à la loi informatique et libertés du 6 janvier 1978, tout traitement de données à caractère personnel nécessite une déclaration à la CNIL.

### 1.1 La déclaration d' I-VAE à la CNIL

L'application I-VAE recueille des données à caractère personnel, de ce fait une déclaration à la CNIL est nécessaire et plus précisément une déclaration sous la forme d'une **déclaration normale**. Cette démarche administrative doit être faite pour chaque académie **au nom du recteur, considéré comme le responsable de traitement**. Toutefois, si vous disposez d'un CIL (correspondant informatique et libertés) dans votre académie, vous devez uniquement l'informer de ce traitement.

**Afin de vous aider dans cette démarche, l'académie de Strasbourg met à votre disposition un tutoriel de déclaration.**

### 1.2 La mention relative au droit d'accès sur les formulaires papiers

Conformément à l'article 32 de la loi informatique et libertés tout recueil de données nécessite d'informer les personnes concernées par cette collecte. Toute personne doit donc avoir connaissance des informations relatives au responsable de traitement et à la finalité de celle-ci.

I-VAE collecte les données relatives aux candidats à partir du site FranceVAE et des éventuels formulaires papiers fournis par les DAVA. Les mentions relatives aux droits d'accès figurent dans le formulaire en ligne de FranceVAE. **Ces mentions doivent aussi figurer sur les formulaires papiers.**

La mention à faire figurer sur votre formulaire papier est la suivante :

*Les informations recueillies font l'objet d'un traitement informatique à destination des services chargés de la VAE (Validation des Acquis de l'Expérience).*

*Ce traitement permet au candidat de s'inscrire à une réunion d'information sur la VAE. Ces informations permettront d'élaborer et de suivre le parcours de la candidature du candidat.*

*Conformément à la loi informatique et libertés du 6 janvier 1978 modifiée en 2004, le candidat bénéficie d'un droit d'accès et de rectification aux informations qui le concernent, et peut exercer son droit en adressant son courrier à l'adresse suivante :*

**L'adresse de votre DAVA**

*Le candidat peut également, pour des motifs légitimes, s'opposer au traitement des données le concernant.*

## II- La loi informatique et libertés

La déclaration de l'application I-VAE à la CNIL constitue une partie des obligations découlant de la loi informatique et libertés. Cette loi énonce un ensemble d'obligations légales : tout manquement est sanctionné par le code pénal, c'est le responsable de traitement qui est pénalement responsable.

**Les responsables et les personnels des DAVA doivent porter une attention toute particulière à :**

### 2.1 La sécurisation du fichier

Le responsable de traitement doit adopter des mesures de sécurité physique (sécurité des locaux) mais aussi adopter des bonnes pratiques en matière de sécurité des systèmes d'information (*Cf. III- La préconisation en matière de sécurité des systèmes d'information*)

**Article 226-17 du code pénal** : Le non-respect de l'obligation de sécurité est sanctionné de 5 ans d'emprisonnement et de 300 000 euros d'amende.

### 2.2 La confidentialité des données

Seules les personnes autorisées, en l'occurrence les personnels des DAVA, peuvent accéder aux données à caractère personnel contenues dans le fichier I-VAE.

**Article 226-22 du code pénal** : La communication d'informations à des personnes non-autorisées est punie de 5 ans d'emprisonnement et de 300 000 euros. La divulgation d'information commise par imprudence ou négligence est punie de 3 ans d'emprisonnement et de 100 000 euros d'amende.

### 2.3 La durée de conservation des informations

Comme indiqué dans le tutoriel de déclaration CNIL de I-VAE, la durée de conservation des données ne doit pas dépasser 5 ans.

**Article 226-20 du code pénal** : La conservation de données pour une durée supérieure à celle qui a été déclarée est sanctionnée de 5 ans d'emprisonnement et de 300 000 euros d'amende.

### 2.4 L'information des personnes

Le responsable de traitement doit permettre aux personnes concernées par des informations qu'il détient d'exercer pleinement leurs droits.

Ces mentions sont à faire figurer sur le formulaire (*Cf. 1.2 La mention relative au droit d'accès sur les formulaires papiers*).

### 2.5 La déclaration du fichier à la CNIL (*Cf. 1.1 La déclaration d'I-VAE à la CNIL*)

**Article 226-16 du code pénal** : le non-accomplissement des formalités auprès de la CNIL est sanctionné de 5 ans d'emprisonnement et de 300 000 euros d'amende.

### 2.6 La finalité du traitement

Les informations recueillies dans I-VAE ne peuvent pas être réutilisées pour une finalité autre que celle pour laquelle elles ont été collectées.

**Article 226-21 du code pénal** : Tout détournement de finalité est passible de 5 ans d'emprisonnement et de 300 000 euros d'amende.

### III- Les préconisations en matière de sécurité des systèmes d'information

Le personnel des DAVA ayant accès aux données à caractère personnel doit, tout d'abord, avoir connaissance des principes de la loi informatique et libertés (Cf. II- La loi informatique et libertés) mais également prendre en considération l'aspect technique de la sécurité des données.

**La sécurisation mise en place par l'académie de Strasbourg pour l'hébergement d'I-VAE est inefficace sans le respect des bonnes pratiques des utilisateurs de chaque académie.**

**Chaque utilisateur doit appliquer les bonnes pratiques suivantes :**

#### 3.1 La sécurisation du poste

Tout personnel ayant accès aux données à caractère personnel, figurant dans l'application I-VAE, doit veiller à respecter les principes de la sécurisation de son poste de travail en :

- Le sécurisant par un **mot de passe fort** (Cf. 3.2 le choix d'un mot de passe fort), personnel et non communiqué (Cf. 3.3 La confidentialité).
- **Verrouillant le poste de travail** ( Ctrl+Alt+Suppr ou touche Windows+L), lorsque le personnel quitte momentanément son poste ainsi que configurer et activer **l'écran de veille avec protection par mot de passe**. En fin de journée, il est conseillé à tout utilisateur d'arrêter le poste de travail.
- **Ne pas communiquer ses codes d'accès.**

#### 3.2 Le choix d'un mot de passe fort

Comme pour le mot de passe de l'accès à votre session de travail, il est impératif de choisir un mot de passe fort et confidentiel (Cf. 3.3 la confidentialité) pour accéder à I-VAE. **Ce mot de passe doit comporter au moins 8 caractères, composé de lettres minuscules et majuscules, de chiffres et de caractères spéciaux :**

- Au moins 2 lettres majuscules
- Au moins 2 lettres minuscules
- Au moins 2 chiffres
- Au moins 2 caractères spéciaux parmi : : ; \_ = \ / ? ^ & ! . @ \$ % # \* ( ) % ~ < > { } [ ]

Nous vous déconseillons toutefois l'usage de caractères accentués.

**Astuce** : Une manière simple de composer un tel mot de passe est de penser à une phrase connue, et de ne garder que les premières lettres de chaque mot. Ensuite on peut transformer les *un/une* par le chiffre 1, les *a* par des @, les *e* par des &, ou tout autre stratagème de ce type, et ponctuer la phrase.

Par exemple : **Qui vole un Oeuf, vole un Bœuf !**

devient : **Qv1O,v1B!**

On a bien 2 chiffres, 2 caractères spéciaux, 2 majuscules (même trois) et 2 minuscules.

#### 3.3 La confidentialité

Les personnels des DAVA sont considérés comme étant les seuls destinataires des données d'I-VAE donc les seuls habilités à consulter ces données. Chaque personnel dispose de son propre mot de passe d'accès et doit porter une attention toute particulière à la confidentialité de son mot de passe que ce soit celui de son poste ou de l'accès à I-VAE. Le mot de passe est propre à chaque personnel et non transmissible, ne le divulguez pas. Une opération réalisée avec votre identifiant est réalisée en votre nom et engage votre responsabilité.

### IV- Pour plus d'informations

Si vous souhaitez disposer d'autres informations relatives à la protection des données ou à la sécurisation de celles-ci vous pouvez joindre le service de la sécurité des systèmes d'information de l'académie de Strasbourg par mail :

[rssi@ac-strasbourg.fr](mailto:rssi@ac-strasbourg.fr) .