

## **CONDITIONS D'UTILISATION MON PROFIL E-GOV**

### **Article 1 - Champ d'application des présentes conditions d'utilisation**

Les présentes conditions d'utilisation règlent la procédure mise en place par l'Administration fédérale pour l'enregistrement, l'identification et l'authentification électroniques d'utilisateurs finaux, citoyens ou non. Par le biais de cette procédure, les utilisateurs finaux peuvent s'enregistrer afin d'accéder de manière sécurisée aux services électroniques de l'Administration et de communiquer électroniquement en toute sécurité avec l'Administration. Il se peut cependant que certaines instances publiques aient recours à d'autres systèmes de gestion électronique des utilisateurs finaux.

### **Article 2 - Accès à la procédure**

L'utilisateur final a accès à la procédure sans que l'on puisse cependant lui garantir que l'accès à la procédure et les services offerts seront en tout temps assurés, ne présenteront aucunes erreurs et ne seront pas perturbés techniquement.

L'accès à la procédure peut, à tout moment, être partiellement ou entièrement bloqué (notamment à des fins de maintenance). Pour autant que ce soit raisonnablement possible, l'utilisateur final sera préalablement tenu informé de telles interruptions.

L'utilisateur final n'aura accès à certains services offerts par l'Administration qu'après avoir suivi la procédure d'enregistrement, d'identification et d'authentification applicable.

Dans ce cadre, l'utilisateur final devra :

- se déclarer d'accord avec les présentes conditions d'utilisation ;
- confirmer que ses données d'identité sont correctes ;
- fournir une adresse e-mail correcte.

Si nécessaire, l'utilisateur final est tenu d'adapter les données le concernant afin qu'elles soient toujours actualisées et correctes.

### **Article 3 - Utilisation de moyens d'authentification**

L'accès de l'utilisateur final à certains services offerts par voie électronique nécessite l'utilisation de moyens d'authentification (eID, nom d'utilisateur et mot de passe, token, ...).

Ces moyens d'authentification, ainsi que les données qui y sont liées, sont strictement personnels et non transmissibles.

Chaque utilisateur final est responsable de la bonne conservation, sécurisation, discrétion et gestion de ses moyens d'authentification et des données qui y sont associées.

L'utilisateur final est responsable du choix d'un mot de passe ou autre code secret sûr.

Si un utilisateur final a connaissance de la perte de son nom d'utilisateur, mot de passe, token, ou autre moyen d'authentification, ou de leur utilisation illicite par des tiers, ou s'il soupçonne une telle perte ou une telle utilisation illicite, il doit immédiatement prendre toutes les mesures nécessaires afin de désactiver le moyen d'authentification comme prescrit à l'article 6 notamment.

En cas de verrouillage de son moyen d'authentification, l'utilisateur final devra en demander un nouveau.

#### **Article 4 - Utilisation de l'adresse e-mail**

L'utilisateur final est responsable du choix de l'adresse e-mail qu'il communique. Il déclare que cette adresse e-mail lui appartient et que des tiers ne peuvent en faire usage sans son autorisation.

L'utilisateur final confirme utiliser régulièrement cette adresse.

#### **Article 5 - Utilisation de la procédure**

Chaque utilisateur final est tenu de :

1. fournir des informations complètes, précises, véridiques et non mensongères ;
2. respecter les dispositions prescrites par voie de loi, règlement, décret, ordonnance ou arrêté de l'autorité fédérale, régionale, locale ou internationale ;
3. s'abstenir de manipuler les informations fournies, de quelque manière que ce soit et avec quelque technique que ce soit.

#### **Article 6 - Procédure en cas de perte d'un moyen d'authentification**

Lorsque l'utilisateur final a perdu son token, il doit le désactiver et peut en demander un nouveau via le menu « Mes moyens d'authentification ». En cas de nouvelle demande, le système générera un nouveau token qui sera envoyé par voie postale traditionnelle à l'adresse officielle de l'utilisateur final, telle que reprise dans le Registre national. L'ancien token sera désactivé le plus rapidement possible et ne sera plus utilisable à partir de ce moment-là.

En cas de perte ou de vol d'une carte d'identité, son titulaire est tenu d'en faire la déclaration au plus vite au service de la Population de sa commune ou au poste de police le plus proche, ou de prendre contact avec le service DocStop du SPF Intérieur.

**Article 7 - Protection de la vie privée**

L'Administration fédérale veille à votre vie privée et, dans ce cadre, agit toujours conformément aux dispositions de la législation belge en matière de vie privée (*Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*).

En utilisant cette procédure d'enregistrement, l'utilisateur final donne explicitement son accord pour l'utilisation de ses données personnelles. Il reconnaît que le traitement de ces données personnelles est pertinent et nécessaire pour permettre une identification et une authentification correctes et sécurisées de manière à pouvoir mettre en place une gestion des utilisateurs sûre et une communication électronique entre l'utilisateur final et l'Administration.

L'utilisateur final donne explicitement son accord pour l'enregistrement de son numéro de Registre national dans le système et reconnaît que la conservation de ce numéro est nécessaire et pertinente pour le bon fonctionnement du système. Fedict dispose à cet égard des habilitations nécessaires émanant du Comité sectoriel du Registre national.

Certaines données d'identification sont consultées dans le Registre national ou le Registre BIS. Fedict dispose des autorisations nécessaires à cette fin.

Fedict est responsable du traitement de ces données à caractère personnel et veille à la confidentialité et à la sécurité des données. Fedict est chargé de répondre aux questions relatives à la protection des données à caractère personnel. Les données à caractère personnel que l'utilisateur final saisit sont envoyées sur Internet via le protocole SSL. Les données à caractère personnel ne sont mises qu'à la disposition d'autres services publics utilisant le service pour identifier et authentifier des utilisateurs finaux et leur donner accès à leurs services en ligne. Le service ne peut être utilisé par les autres services publics que s'ils disposent des autorisations nécessaires délivrées par le Comité sectoriel du Registre national.

L'utilisateur final a toujours le droit de mettre fin, en se désinscrivant, au traitement des données à caractère personnel qu'il a communiquées.

La piste d'audit (*audit trail*) relative à la vie privée fait en sorte que les identifications et tentatives d'identifications peuvent être reconstruites afin de respecter l'obligation légale (article 16, §4, de la loi du 8 décembre 1992) qui impose de sécuriser suffisamment les données à caractère personnel.

Fedict utilise des cookies pour améliorer les performances du site web, des cookies fonctionnels pour la convivialité d'utilisation et des cookies de session temporaire nécessaires à l'authentification pendant la session. Vous pouvez refuser les cookies mais, dans ce cas, certaines parties de nos sites web ne fonctionneront pas ou pas de façon optimale.

#### Cookies nécessaires

Ces cookies sont indispensables pour contrôler votre identité de manière sûre et, sur cette base, vous donner accès aux applications auxquelles vous souhaitez accéder.

#### Cookies fonctionnels

Les cookies fonctionnels permettent d'améliorer le fonctionnement des sites web et la convivialité d'utilisation. Fedict utilise des cookies pour retenir votre langue de prédilection.

#### Cookies pour performances du site web

Fedict utilise des « load balancing cookies ». Ils sont utilisés sur des sites web qui sont beaucoup visités et servent à partager les charges des demandes entre plusieurs réseaux et serveurs distincts.

Il est possible de refuser des cookies par le biais des paramètres du navigateur.

### **Article 8 - Définitions**

Aux fins des présentes conditions d'utilisation, les notions ci-dessous sont définies comme suit :

- **Enregistrement** - Le processus par lequel une personne se fait inscrire – en suivant une procédure préétablie – dans une liste, et fait dès lors savoir qu'elle souhaite faire usage d'un certain service.
- **Identification** - Un processus qui est utilisé pour constater l'identité d'une certaine personne.
- **Authentification** - Processus utilisé pour confirmer l'identité d'une certaine personne. Une personne peut par exemple, en fournissant certaines données confidentielles qui ne sont connues que d'elle (p. ex. un mot de passe choisi par elle-même), confirmer qu'elle est bel et bien la personne qu'elle prétend être.