|  |  |  |
| --- | --- | --- |
|  |  |  |

|  |  |
| --- | --- |
|  | Cartouche destiné à recevoir le cachet société du titulaire de l’accord-cadre et la signature d'une personne physique ayant pouvoir pour engager la responsabilité de la personne morale dudit titulaire |

**CAHIER DES CLAUSES ADMINISTRATIVES PARTICULIERES  
Annexe II  
Déclaration individuelle d’engagement  
et de reconnaissance de responsabilité**

Expertise indépendante de la solution de vote électronique  
mise en œuvre pour les élections professionnelles en 2026 et en 2027   
au ministère de l’éducation nationale et de l’enseignement supérieur et de la recherche et au ministère de sports, de la jeunesse et de la vie associative

Sommaire

[1. Avertissements 2](#_Toc191899984)

[2. Identification du signataire 2](#_Toc191899985)

[3. Déclarations 3](#_Toc191899986)

[4. Engagements 3](#_Toc191899987)

[5. Reconnaissance de responsabilité 5](#_Toc191899988)

# Avertissements

Le secrétariat général des ministères de l’éducation nationale, de l’enseignement supérieur et de la recherche d’une part, et des sports, de la jeunesse et de la vie associative d’autre part, est désigné dans le présent document sous l’appellation « ministère » ou « ministères » ou encore « administration ».

Le titulaire de l’accord-cadre d’expertise indépendante doit signer l’annexe I de sécurité au CCAP de cet accord-cadre. A ce titre, ce titulaire doit faire signer par tous les agents, appelés sous sa responsabilité à intervenir dans le cadre de l'exécution des prestations de cet accord-cadre, la présente déclaration individuelle d’engagement et de reconnaissance de responsabilité ci-après désignée par « ERR ».

Lesdits agents vont ainsi attester d’une part, avoir pris connaissance des dispositions de l’instruction générale interministérielle n°1300 (IGI1300) et des articles 413-9 à 413-12 du code pénal, et d’autre part, qu'ils n'ont pas, sous peine de poursuite pénale, à connaître ou détenir des informations sensibles de l’administration ou des informations couvertes par le secret de la défense nationale.

Cet ERR est notamment relatif au bon respect des obligations de confidentialité, de protection des données à caractère personnel ou sensibles et des mesures de sécurité en vigueur aux ministères. L’accès aux systèmes d’information des ministères doit se faire dans le strict respect de la législation et, en particulier, celle applicable au respect des personnes et de la propriété intellectuelle ainsi qu’aux actes de fraude, de détournement et de malveillance informatique.

# Identification du signataire

|  |  |
| --- | --- |
| **Nom et prénom de la personne physique signataire** |  |
| **Qualité du signataire** Cette information doit permettre d'établir à quel(s) titre(s) le signataire da intervenir dans le cadre du marché et de déterminer si le signataire est agent du titulaire ou d’un de ses sous-traitants |  |
| **Identification du titulaire pour le compte duquel le signataire intervient** |  |
| **Référence de l’accord-cadre liant le titulaire et l’administration** |  |

# Déclarations

**Je soussigné(e) reconnais avoir été sensibilisé par le titulaire responsable de l’exécution des prestations de l’accord-cadre et de ce fait avoir pleinement connaissance :**

* Que l’autorisation d’accès aux locaux de l'administration est conditionnée à l'obtention d'une autorisation d'accès délivrée après enquête diligentée par le service de sécurité compétent ;
* Que ce droit d’accès est strictement personnel, incessible et limité dans le temps ;
* Que l’administration peut, à tout instant, demander à contrôler sans restriction l’utilisation qui est faite de ce droit d’accès ;
* Que mon activité s’exerce en zone protégée telle que définie par l’article 5.3.1.1 de l’IGI1300 ;
* Que toute éventuelle action contraire aux règles édictées doit être immédiatement signalée à la DGRH et à sa voie fonctionnelle SSI représentée par son Responsable de Sécurité des Systèmes d’Information (RSSI) et son Officier de sécurité ;
* Des dispositions générales relatives à la réglementation et à la législation française en vigueur :
  + Dans le domaine de la sécurité des systèmes d'information et plus particulièrement à la fraude informatique, notamment les articles 323-1 à 321-3 du code pénal,
  + Dans le domaine du secret de la défense nationale et notamment des articles 413-9 à 413-12 du code pénal,
  + Et dans le domaine du droit de la propriété intellectuelle et notamment les articles L.111-1, L.112-1 à L.112-3 et L.342-1 du code de la propriété intellectuelle ;
* Qu’un dispositif, reposant notamment sur la journalisation des notifications techniques et de sécurité, permet d’assurer la traçabilité de l’ensemble des actions menées sur le système d’information de l’Administration.

# Engagements

**Je m’engage par ailleurs à :**

* Suivre et respecter les dispositions décrites dans l’annexe I du CCAP de l’accord-cadre, relative à la protection des informations, à la confidentialité et aux mesures de sécurité, qui a été signée par le titulaire et qui a été portée à ma connaissance par ce titulaire ;
* Respecter l’obligation de discrétion professionnelle pour tous les faits, informations ou documents dont j’aurais connaissance dans l'exercice ou à l'occasion de l'exercice de ma mission ;
* Ne divulguer, ou ne communiquer à un tiers, en aucun cas des informations ou données tant personnelles que professionnelles que je pourrais être amené(e) à apprendre dans l’exercice de ma mission ;
* Ne pas reproduire de quelque manière que ce soit, stocker sur quelque support que ce soit, diffuser via quelque média que ce soit, modifier, altérer ou détruire toute donnée ou information dont je pourrais avoir connaissance à d’autres fins que celles de l’exercice de ma mission ;
* Respecter le principe fondamental du « besoin d'en connaître » et ainsi de ne pas tenter d'accéder, de reproduire, de stocker, de copier, de diffuser, de modifier, d'altérer ou de détruire toute information dont je ne suis pas supposé avoir connaissance dans l’exercice de ma mission. Le « besoin d’en connaître » est défini par l’IGI1300 comme la « *nécessité impérieuse de prendre connaissance d’une information dans le cadre de l’exercice d’une fonction ou l’accomplissement d’une mission.* ».

**Si, à l’occasion de l’exécution de ma mission, je dispose d’un accès à un système d’information de l’administration et, par conséquent, d’un compte nominatif, je m’engage également à :**

* Ne pas tenter d’introduire, d’installer et de connecter tout moyen informatique matériel ou logiciel, et notamment tout appareil électronique communicant ou non, personnel ou du titulaire, au système d’information du ministère sans avoir reçu préalablement l’autorisation formelle de l’administration ;
* Ne pas modifier sans autorisation la configuration des moyens mis à ma disposition par l’administration pour l’exercice de ma mission ;
* Ne pas introduire dans le système d’information du ministère, y tester ou y utiliser des supports informatique ou médias dont l’origine m’est inconnue, douteuse ou incertaine ;
* Ne pas perturber ou interrompre le fonctionnement normal du système d’information du ministère ou de l’un de ses composants ;
* Ne pas me livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des services, applications et moyens auxquels j’ai accès ;
* Ne pas générer volontairement ou involontairement des perturbations du système d’information du ministère que ce soit par des manipulations anormales ou par l’introduction illicite de composants matériels ou logiciels contrefaits ou piratés ;
* Ne pas mettre à la disposition d’utilisateurs non autorisés un accès privilégié aux ressources informatiques, données ou services du ministère et de ses partenaires quelle que puisse être la nature du partenariat.

**Je m’engage, conformément aux articles 34 et 35 de la loi du 6 janvier 1978 modifiée relative à l’informatique, aux fichiers et aux libertés ainsi qu’aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016 à** prendre toutes précautions conformes aux usages et à l’état de l’art dans le cadre du marché et de ma mission afin de protéger la confidentialité des données à caractère personnel auxquelles j’ai accès, et en particulier d’empêcher qu’elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

**Je m’engage en particulier à :**

* Ne pas utiliser les données à caractère personnel auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;
* Ne divulguer ces données à caractère personnel qu’aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu’il s’agisse de personnes privées, publiques, physiques ou morales ;
* Ne faire aucune copie de ces données à caractère personnel sauf à ce que cela soit nécessaire à l’exécution des prestations de l’accord-cadre et de ma mission ;
* Prendre toutes les mesures conformes aux usages et à l’état de l’art dans le cadre de ma mission afin d’éviter l’utilisation détournée ou frauduleuse de ces données à caractère personnel ;
* Prendre toutes précautions conformes aux usages et à l’état de l’art pour préserver la sécurité physique et logique de ces données à caractère personnel ;
* M’assurer, dans la limite de ma mission, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données à caractère personnel ;
* En cas de cessation de ma qualité d’intervenant du titulaire, quels qu’en soient les motifs, restituer intégralement les données, fichiers informatiques et tout support d’information relatif à ces données à caractère personnel.

Cet engagement de confidentialité, en vigueur pendant toute la durée de ma mission dans le cadre du marché, demeurera effectif, sans limitation de durée après la cessation de de ma qualité d’intervenant du titulaire, quelle qu’en soit la cause, dès lors que cet engagement concerne l’utilisation et la communication de données à caractère personnel des ministères.

# Reconnaissance de responsabilité

**Je déclare être pleinement conscient(e) de mes responsabilités et de la portée pénale et juridique des déclarations et engagements qui sont énoncés dans le présent document. Je reconnais être informé(e) des conséquences pénales, notamment au regard des articles 226-16 à 226-24 du code pénal, et contractuelles qui pourraient résulter de la non application des procédures et dispositions édictées ci‑dessus.**

|  |  |
| --- | --- |
| Cette signature doit être précédée par les mentions :   * "Fait à :" suivie de l'identification du lieu où a été apposée la signature ; * "Le : " suivie de la date de la signature.   En application des dispositions de l'article 1367 du code civil, cette signature manifeste le consentement du signataire au contenu de la présente déclaration individuelle et engagement de reconnaissance de responsabilité. | **Fait à                                   Le                                                   Le signataire** |

Extraits du code pénal relatifs aux dispositions générales touchant à la fraude informatique.

**Article 323-1**

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

**Article 323-2**

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

**Article 323-3**

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

**Article 323-3-1**

Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Extraits du code pénal relatifs aux dispositions générales touchant aux atteintes au secret de la défense nationale.

**Article 413-9**

Présentent un caractère de secret de la défense nationale au sens de la présente section les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès.

Peuvent faire l'objet de telles mesures les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers dont la divulgation ou auxquels l'accès est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale.

Les niveaux de classification des procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers présentant un caractère de secret de la défense nationale et les autorités chargées de définir les modalités selon lesquelles est organisée leur protection sont déterminés par décret en Conseil d'Etat.

**Article 413-10**

Est puni de sept ans d'emprisonnement et de 100 000 euros d'amende le fait, par toute personne dépositaire, soit par état ou profession, soit en raison d'une fonction ou d'une mission temporaire ou permanente, d'un procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier qui a un caractère de secret de la défense nationale, soit de le détruire, détourner, soustraire ou de le reproduire, soit d'en donner l'accès à une personne non qualifiée ou de le porter à la connaissance du public ou d'une personne non qualifiée.

Est puni des mêmes peines le fait, par la personne dépositaire, d'avoir laissé accéder à, détruire, détourner, soustraire, reproduire ou divulguer le procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier visé à l'alinéa précédent. Lorsque la personne dépositaire a agi par imprudence ou négligence, l'infraction est punie de trois ans d'emprisonnement et de 45 000 euros d'amende.

**Article 413-11**

Est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende le fait, par toute personne non visée à l’article 413-10 de :

1. S'assurer la possession d'un renseignement, procédé, objet, document, donnée informatisée ou fichier qui présente le caractère d'un secret de la défense nationale ;
2. Détruire, soustraire ou reproduire, de quelque manière que ce soit, un tel renseignement, procédé, objet, document, donnée informatisée ou fichier ;
3. Porter à la connaissance du public ou d'une personne non qualifiée un tel renseignement, procédé, objet, document, donnée informatisée ou fichier.

**Article 413-12**

La tentative des délits prévus au premier alinéa de l’article 413-10 et à l’article 413-11 est punie des mêmes peines.

Extraits du code de la propriété intellectuelle.

**Article L.111-1 (extrait)**

L'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous. Ce droit comporte des attributs d'ordre intellectuel et moral ainsi que des attributs d'ordre patrimonial, qui sont déterminés par les livres Ier et III du présent code.

L'existence ou la conclusion d'un contrat de louage d'ouvrage ou de service par l'auteur d'une œuvre de l'esprit n'emporte pas dérogation à la jouissance du droit reconnu par le premier alinéa, sous réserve des exceptions prévues par le présent code. Sous les mêmes réserves, il n'est pas non plus dérogé à la jouissance de ce même droit lorsque l'auteur de l'œuvre de l'esprit est un agent de l'Etat, d'une collectivité territoriale, d'un établissement public à caractère administratif, d'une autorité administrative indépendante dotée de la personnalité morale, de la Banque de France, de l'Institut de France, de l'Académie française, de l'Académie des inscriptions et belles-lettres, de l'Académie des sciences, de l'Académie des beaux-arts ou de l'Académie des sciences morales et politique.

**Article L.112-1**

Les dispositions du présent code protègent les droits des auteurs sur toutes les œuvres de l'esprit, quels qu'en soient le genre, la forme d'expression, le mérite ou la destination.

**Article L112-2 (extrait)**

Sont considérés notamment comme œuvres de l'esprit au sens du présent code :

[…]

1. Les logiciels, y compris le matériel de conception préparatoire ;

[…]

**Article L112-3**

Les auteurs de traductions, d'adaptations, transformations ou arrangements des œuvres de l'esprit jouissent de la protection instituée par le présent code sans préjudice des droits de l'auteur de l'œuvre originale. Il en est de même des auteurs d'anthologies ou de recueils d'œuvres ou de données diverses, tels que les bases de données, qui, par le choix ou la disposition des matières, constituent des créations intellectuelles.

On entend par base de données un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen.

**Article L342-1**

Le producteur de bases de données a le droit d'interdire :

1. L'extraction, par transfert permanent ou temporaire de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu d'une base de données sur un autre support, par tout moyen et sous toute forme que ce soit ;
2. La réutilisation, par la mise à la disposition du public de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base, quelle qu'en soit la forme.

Ces droits peuvent être transmis ou cédés ou faire l'objet d'une licence. Le prêt public n'est pas un acte d'extraction ou de réutilisation.