

## **PROTECTION DES DONNEES PERSONNELLES**

**Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, applicable à compter du 25 mai 2018 (le règlement européen sur la protection des données) et loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles**

Objet du marché :

### **Tierce maintenance applicative (TMA) et maintien en conditions opérationnelles (MCO) de la plateforme Annuaire**

---

#### **Annexe n° 2 au CCAP**

#### **PROTECTION DES DONNEES PERSONNELLES**

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, applicable à compter du 25 mai 2018 (le règlement européen sur la protection des données) et loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles

Le titulaire du présent marché est responsable du traitement des données à caractère personnel.

Il fixe les finalités et les moyens du traitement.

Pour l'exécution du marché public, en cas de traitement de données à caractère personnel, le titulaire, et le cas échéant ses sous-traitants, sont tenus au respect de la réglementation en vigueur applicable au traitement de données à caractère personnel et, notamment le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après, « règlement général sur la protection des données » ou RGPD) et la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Le cas échéant, le titulaire apporte à l'acheteur, avant la mise en application du traitement, des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen et garantisse la protection des droits des personnes concernées.

Dès la notification du marché, il communique à l'acheteur l'identité et les coordonnées (téléphone et mail) de son délégué à la protection des données (DPD).

#### **Précisions terminologiques :**

Dans le cas présent, le responsable de traitement au sens du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après, « règlement général sur la protection des données » ou RGPD) est le titulaire du marché et le sous-traitant est l'Administration.

### **Nature, durée, finalité et description du traitement de données à caractères personnel :**

Le titulaire est autorisé à traiter pour le compte de l'acheteur, les données à caractère personnel nécessaires pour fournir la ou les prestations (s) suivante (s) :

- Maintien en conditions opérationnelles et de sécurité des annuaires Anais, Proxy, Anael, Angie et MSG

Les données à caractère personnel sont traitées pour une durée de :

- Correspondante à la durée d'exécution du présent marché public

Nature des opérations réalisées sur les données :

- Consultation, modification et suppression

La ou les finalité(s) du traitement sont les suivantes :

- Identification/Authentification et fourniture d'identité aux intranets
- Fourniture de données aux applications (Recherche et consultation des coordonnées des agents)

Les types de données à caractère personnel traitées sont les suivantes :

- Etat civil et identité : Civilité, Nom, Prénom et photographie
- Données de connexion : adresse IP, logs
- Vie professionnelle : Identifiant ministériel, mail, Identifiant de connexion, Bâtiment, adresse du bâtiment, N° bureau, courriel, N° de téléphone, Grade, fonction, attribution, affectation et certificat de signature et de chiffrement.

Les catégories de personnes concernées par les données sont les suivantes :

- Les agents du ministère des MEF : Tous les agents ayant besoin d'accéder au système d'information de l'administration centrale : titulaires, contractuels, apprentis, stagiaires, vacataires, ...
- Les prestataires : Les externes qui travaillent pour l'administration centrale et ayant besoin d'accéder au SI de l'administration centrale

### **Concernant les données sensibles :**

Si le traitement porte sur des données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, ou des données relatives aux condamnations pénales et aux infractions (« données sensibles »), le sous-traitant applique des limitations spécifiques et/ou des garanties supplémentaires.

### **Concernant la mise en œuvre du traitement :**

- a) Obligations du titulaire vis-à-vis de l'acheteur

Le titulaire du marché public s'engage, notamment, à :

1. traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet du présent marché public ;
2. traiter les données conformément aux instructions documentées de l'acheteur figurant [à compléter : en annexe ou dans les documents particuliers du présent marché]. Si le titulaire considère qu'une instruction est donnée en violation du règlement général sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en informe immédiatement l'acheteur ;
3. Si le titulaire est tenu de procéder à un transfert de données vers un pays tiers (hors de l'Union européenne) ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer l'acheteur de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information ;

Les données transférées vers un pays tiers doivent bénéficier d'un degré de protection équivalent à celui garanti par le RGPD au sein de l'Union européenne. Il est rappelé que tout transfert de données à caractère personnel, au bénéfice de toute entité et notamment de pays tiers ou d'organisations internationales, qui ne serait pas strictement conforme à la réglementation française ou européenne est formellement prohibé.

A défaut de pouvoir garantir le respect de ces exigences en cas de transfert de données à caractère personnel vers un pays tiers, le titulaire suspend tout transfert et se rapproche de l'acheteur pour envisager, le cas échéant, l'adaptation des modalités d'exécution du marché permettant le respect des exigences du RGPD.

Si les modalités d'exécution ne peuvent être adaptées, l'acheteur procède à la résiliation du marché pour motif d'intérêt général dans les conditions prévues par le CCAG de référence.

4. garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent marché public ;
5. veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent marché public :
  - s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
  - reçoivent la formation nécessaire en matière de protection des données à caractère personnel.
6. prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut.

b) Sous-traitance des activités de traitement

Lorsque le titulaire (qui est, pour rappel, sous-traitant au sens RGPD), fait appel à un sous-traitant (au sens de la commande publique) pour mener des activités de traitement spécifiques, il informe préalablement et par écrit l'acheteur (le responsable de traitement au sens du RGPD). Cette information doit indiquer clairement la nature des activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Cette sous-traitance ne peut être effectuée que si l'acheteur n'a pas émis d'objection pendant le délai de 21 jours à compter

de la date de réception de la demande en application des dispositions de l'article R.2193-4 du code de la commande publique.

Afin d'obtenir l'acceptation et l'agrément de l'acheteur, le titulaire doit présenter son sous-traitant par le biais de l'acte spécial de sous-traitance, dont les formalités sont comprises dans le formulaire DC4 ou tout autre document équivalent.

Le formulaire DC4 est téléchargeable sur :

<https://www.economie.gouv.fr/daj/formulaires-declaration-du-candidat>

Le sous-traitant est tenu de respecter les obligations du présent marché public pour le compte et selon les instructions de l'acheteur. Il appartient au titulaire de s'assurer que le sous-traitant présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences de la législation et de la réglementation en vigueur sur la protection des données.

Le titulaire demeure pleinement responsable, à l'égard de l'acheteur, de l'exécution des obligations du sous-traitant conformément au contrat conclu avec le sous-traitant ultérieur. Le titulaire informe l'acheteur de tout manquement du sous-traitant à ses obligations contractuelles.

#### c) Droit d'information et exercice des personnes concernées par le traitement

Il appartient au titulaire de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

La formulation et le format de l'information doivent être convenus avec l'acheteur avant la collecte de données.

Le titulaire doit répondre, au nom et pour le compte de l'acheteur et dans les délais prévus par le règlement général sur la protection des données, aux demandes des personnes concernées en cas d'exercice de leurs droits.

Le titulaire doit pouvoir garantir, pendant toute la durée des prestations, que l'intégralité des données à caractère personnel qu'il traite dans le cadre de l'exécution du marché en qualité de sous-traitant RGPD sont traitées et plus généralement rendues accessibles exclusivement au sein :

- De l'Espace économique européen ;
- D'un État tiers bénéficiant d'une décision d'adéquation au sens de l'article 45 du RGPD ;
- Ou, à défaut, que les transferts résultant de la réalisation des Prestations sont encadrés par des garanties appropriées ou des règles d'entreprise contraignantes au sens des articles 46 et 47 du RGPD, le cas échéant complétées par des mesures supplémentaires visant à garantir qu'il ne pourra pas y être fait échec dans l'État tiers de destination, dans le strict respect de la jurisprudence.

La garantie du titulaire sur ce point doit non seulement couvrir l'hébergement des données, mais également toutes les opérations de traitement réalisées par le titulaire ou par les sous-traitants RGPD ultérieurs auxquels pourraient le cas échéant être confiées certaines opérations de traitement (telles que notamment maintenance, assistance...).

Le titulaire doit ainsi pouvoir garantir que les données traitées ne peuvent pas être rendues accessibles à des destinataires, y compris des autorités administratives ou judiciaires, situés hors de l'Espace économique européen sans que soit respecté le droit applicable, et en particulier le RGPD. Le titulaire détaillera les moyens mis en place pour y répondre.

d) Notification des violations de données à caractère personnel

Le titulaire notifie à l'acheteur toute violation de données à caractère personnel dans un délai de 24 heures après en avoir pris connaissance et par le moyen suivant :

- Courriel au chef de projet désigné par l'Administration.

Cette notification est accompagnée de toute documentation utile afin de permettre à l'acheteur, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente (en l'occurrence, à la Commission nationale de l'informatique et des libertés, CNIL) si possible 72 heures au plus tard après en avoir pris connaissance.

Après accord écrit de l'acheteur, le titulaire notifie à l'autorité de contrôle compétente, au nom et pour le compte de l'acheteur, les violations de données à caractère personnel dans un délai maximum de 24 heures à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

La notification contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, 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 l'acheteur 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.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Après accord écrit de l'acheteur, le titulaire communique, au nom et pour le compte de l'acheteur, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, 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 l'acheteur 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 ;
- Aide du titulaire dans le cadre du respect par l'acheteur de ses obligations.

Le titulaire aide l'acheteur :

- à la réalisation d'analyses d'impact relative à la protection des données ;
- à la réalisation de la consultation préalable de l'autorité de contrôle.

Le titulaire met à la disposition de l'acheteur la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre, le cas échéant, la réalisation d'audits, y compris des inspections, par l'acheteur ou un auditeur mandaté par lui, et contribuer à ces audits.

e) Mesures de sécurité

Le titulaire met en œuvre les mesures de sécurité suivantes :

- la pseudonymisation et le chiffrement des données à caractère personnel
- les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- les moyens 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 ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement

f) Sort des données

Au terme de l'exécution du présent marché public, l'acheteur informe le titulaire de sa décision relative au sort des données. L'acheteur peut demander au titulaire de :

- détruire toutes les données à caractère personnel ;
- renvoyer toutes les données à caractère personnel à l'acheteur ou au tiers désigné par l'acheteur.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction

g) Délégué à la protection des données

Dès la notification du marché public, l'acheteur communique au titulaire le nom et les coordonnées de son délégué à la protection des données.

#### h) Registre des activités de traitement

Le titulaire tient par écrit un registre de toutes les activités de traitement effectuées pour le compte de l'acheteur comprenant :

1. le nom et les coordonnées de l'acheteur pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
2. les catégories de traitements effectués pour le compte de l'acheteur ;
3. le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement général sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
4. dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, notamment, selon les besoins :
  - la pseudonymisation et le chiffrement des données à caractère personnel ;
  - des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
  - des moyens 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 ;
  - une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ;