



Pouvoir Adjudicateur :

Agence de services et de paiement (ASP)

2, rue du Maupas

87 040 LIMOGES cedex 1

Annexe n° 1 du CCAP
Protection des données personnelles

MP26-12

Assistance à maîtrise d'œuvre pour des missions en lien avec les recettes informatiques.

SOMMAIRE

Article 1. Contexte général.....	3
Article 2. Obligations du titulaire vis-à-vis de l'ASP.....	3
2.1 Engagement du titulaire	3
2.2 Délégué à la protection des données.....	3
2.3 Droit d'information des personnes	4
2.4 Mesures de sécurité.....	4
2.5 Registre des catégories d'activités de traitement.....	4
2.6 Sort des données.....	5
Article 3. Documentation.....	5
Article 4. Obligations l'ASP vis-à-vis du titulaire	5

Article 1. Contexte général

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le titulaire s'engage à effectuer pour le compte de l'ASP les opérations de traitement de données à caractère personnel définies ci-après.

Dès la notification du marché, une réunion de travail sera organisée afin de préciser au titulaire du marché :

- la nature des opérations réalisées sur les données,
- la ou les finalité(s) du traitement, les données à caractère personnel traitées,
- la description des traitements,
- les catégories de personnes concernées, le mode d'accès et de manipulation des informations nécessaires à la finalité des prestations, ainsi que les informations nécessaires suivantes à la bonne exécution des dispositions prévues ci-dessous.

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après, « le règlement européen sur la protection des données ») et la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée.

Dans tous les cas, le titulaire du présent marché sera sous-traitant de l'ASP au sens du Règlement général européen sur la protection des données (RGPD). A ce titre, le titulaire rendra compte exclusivement à l'ASP, qu'elle soit responsable de traitement ou sous-traitant d'un donneur d'ordre.

Article 2. Obligations du titulaire vis-à-vis de l'ASP

2.1 Engagement du titulaire

Le titulaire s'engage à :

- respecter les dispositions relatives à la sous-traitance (les modalités de recours à la sous-traitance restant fixées par le CCAP du présent marché) ;
- traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de prestation au titre du marché
- traiter les données conformément aux instructions de l'ASP. Si le titulaire considère qu'une instruction constitue une violation du règlement européen 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'ASP ;
- garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent marché ;
- veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent marché :
 - o s'engagent à respecter la confidentialité prévue au CCAP,
 - o reçoivent la formation nécessaire en matière de protection des données à caractère personnel,
 - o prennent 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.
- mettre en place les moyens nécessaires à la protection des données (exemple : logiciel antivirus, pare-feux, environnements sécurisés...).

2.2 Délégué à la protection des données

Le titulaire communique à l'ASP le nom et les coordonnées de son délégué à la protection des données (DPO), s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données.

2.3 Droit d'information des personnes

Lorsque les personnes concernées exercent leurs droits auprès du titulaire, celui-ci doit transmettre les demandes à l'ASP par courrier électronique dès réception (à l'adresse protectiondesdonnees@asp.gouv.fr).

Notification des violations de données à caractère personnel

Le titulaire notifie à l'ASP toute violation de données à caractère personnel dans un délai maximum de 48 heures après en avoir pris connaissance et par courrier électronique à l'adresse protectiondesdonnees@asp.gouv.fr.

Cette notification est accompagnée de toute documentation utile afin de permettre à l'ASP, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

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 qu'il est proposé 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.

Les personnes concernées par la violation en seront informées par l'ASP.

2.4 Mesures de sécurité

Le titulaire s'engage à mettre en œuvre les mesures de sécurité prévues au CCAP. Le cas échéant, il s'engage à mettre en place :

- 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 garantir la sécurité des systèmes d'information et des locaux hébergeant les données ;
- 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 ;

2.5 Registre des catégories d'activités de traitement

Le titulaire déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte de l'ASP comprenant notamment :

- le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
- les catégories de traitements effectués pour le compte du responsable du traitement ;
- dans la mesure du possible, en application des clauses de sécurité du CCAP, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
 - o les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
 - o 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 ;
 - o une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2.6 Sort des données

Au terme des prestations couvertes par le présent marché, le titulaire s'engage à :

- renvoyer toutes les données à caractère personnel à l'ASP ;
- détruire toutes les copies existantes dans ses systèmes d'information et sur tout support (numérique, papier...);
- justifier par écrit de la destruction de l'ensemble des données concernées.

Article 3. Documentation

Le titulaire met à la disposition de l'ASP la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

Article 4. Obligations l'ASP vis-à-vis du titulaire

L'ASP s'engage à :

- fournir au titulaire les informations nécessaires à la description et à la réalisation du traitement ;
- documenter par écrit toute instruction concernant le traitement des données par le titulaire ;
- veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du titulaire ;
- superviser le traitement, y compris réaliser les audits et les inspections auprès du titulaire.