ANNEXE II – PROTECTION DES DONNEES A CARACTERE PERSONNEL

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable aux traitements de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 et la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 dite directive « police-justice ».

Dans le cas où le titulaire a accès à des données à caractère personnel lors de la réalisation des prestations, il agit en qualité de sous-traitant au sens de l'article 4 du RGPD et de l'article 22 de la directive « police-justice », et ce pour le compte de l'administration qui demeure le responsable de traitement.

La présente annexe a pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

DESCRIPTION DU TRAITEMENT FAISANT L'OBJET DE LA SOUS-TRAITANCE

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour l'exécution du présent accord-cadre.

La nature des opérations réalisées sur les données correspond à l'identification des utilisateurs et de leurs matériels.

La finalité du traitement est la mise en place d'une connexion sécurisée à la plateforme.

Les données à caractère personnel traitées sont les identifiants correspondants à chaque utilisateur et au matériel et l'ensemble des données attachées à la sécurité de ces connexions.

Les catégories de personnes concernées sont les utilisateurs de la plateforme, agents du ministère de l'intérieur.

Pour l'exécution du service objet du présent contrat, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires suivantes : toutes données en rapport avec les connexions des utilisateurs (date de connexion, durée, fréquence, lieu de connexion).

SÉCURITÉ

Le responsable de traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

- 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.

OBLIGATIONS DU SOUS-TRAITANT VIS-À-VIS DU RESPONSABLE DE TRAITEMENT

Le sous-traitant s'engage à :

1. traiter les données **uniquement pour la ou les seule(s) finalité(s)** qui fait/font l'objet de la sous-traitance.

2. Traiter les données **conformément aux instructions documentées** du responsable de traitement. Si le sous-traitant 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 États membres relative à la protection des données, il en **informe immédiatement** le responsable de traitement. En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers 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 le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

3. garantir la **confidentialité** des données à caractère personnel traitées dans le cadre du présent accord-cadre.

4. veiller à ce que les **personnes autorisées à traiter les données à caractère personnel** en vertu du présent accord-cadre :

- 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.

5. 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.**

6. **La sous-traitance**

Le sous-traitant, titulaire de l'accord-cadre, peut faire appel à un autre sous-traitant (ci-après, « ***le sous-traitant ultérieur*** ») pour mener des activités de traitement spécifiques. Dans ce cas, il s'engage notamment à présenter à l'administration, les entreprises auxquelles il envisage de confier la réalisation d'activités de traitement spécifiques. Pour ce faire, il remplit une déclaration relative à la présentation d'un sous-traitant ultérieur, en vertu de l'article L. 2193-5 du code de la commande publique (DC4). En cas d'accord, l'administration accepte le sous-traitant proposé et agréer ses conditions de paiement.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent accord-cadre pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur 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 du RGPD et/ou de la directive « police-justice ». Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

7. **Le droit d'information des personnes concernées**

Il appartient au responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données en fonction de la catégorie de traitement. L'information fait l'objet d'une diffusion lors de la connexion des utilisateurs par l'intermédiaire d'une fenêtre « pop-up » rappelant la collecte des données lors de la première connexion de la journée au service.

8. **L'exercice des droits des personnes**

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage) dans le cadre du RGPD.

Lorsque le traitement relève de la directive « police-justice », l'exercice des droits des personnes fait l'objet de mesures spécifiques compte tenu de la finalité du traitement.

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique au représentant du responsable de traitement.

9. **Notification des violations de données à caractère personnel**

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance et par tout moyen. Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

10. **Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations**

Le sous-traitant aide le responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données.

Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

11. **Le sort des données**

Dans un délai d'un (1) mois calendaire avant la date de fin de l'accord-cadre, le titulaire interroge le responsable de traitement sur le sort des données traitées. Au choix du responsable de traitement, le sous-traitant s'engage à :

- détruire toutes les données à caractère personnel ;
- à renvoyer toutes les données à caractère personnel au responsable de traitement ;

- à renvoyer les données à caractère personnel au sous-traitant désigné par le responsable de traitement.

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.

12. **Le délégué à la protection des données**

Le sous-traitant communique au responsable de traitement **le nom et les coordonnées de son délégué à la protection des données**, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données.

13. **Registre des catégories d'activités de traitement**

Le sous-traitant déclare **tenir par écrit un registre** de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement comprenant :

- 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 ;
- 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 européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;

- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :

    o la pseudonymisation et le chiffrement des données à caractère personnel ;

    o des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

    o 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 ;

    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.

14. Documentation

Le sous-traitant met à la disposition du responsable de traitement, dans le délai fixé par la demande, 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.

OBLIGATIONS DU RESPONSABLE DE TRAITEMENT VIS-À-VIS DU SOUS-TRAITANT

Le responsable de traitement s'engage à :

- fournir au sous-traitant les données à caractère personnel nécessaires pour l'exécution du présent accord-cadre ;
- documenter par écrit toute instruction concernant le traitement des données par le sous-traitant ;
- veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement de la part du sous-traitant ;
- superviser le traitement, y compris réaliser, le cas échéant des audits et des inspections auprès du sous-traitant.