



MINISTÈRE DE L'INTÉRIEUR

*Liberté
Égalité
Fraternité*



l'Europe se mobilise



**Direction de l'évaluation de la performance, de l'achat, des finances et de l'immobilier
Sous-direction de l'achat et du suivi de l'exécution des marchés
Bureau des marchés SIC et conseil**

ANNEXE IX : Protection des données à caractère 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 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 (RGPD).

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 des articles 4 et 28 du RGPD, 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, titulaire de l'accord-cadre relatif à la conception, au développement, à la fourniture, au déploiement et la maintenance de kiosques biométriques de pré-enregistrement des voyageurs notamment dans le cadre du système européen d'entrées – sorties, s'engage à effectuer pour le compte du responsable de traitement, l'Etat, les opérations de traitement de données à caractère personnel définies ci-après.

ARTICLE 1.DESCRPTION 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 est l'enregistrement, la consultation, l'effacement, la mise à jour, le stockage des données.

Les finalités du traitement sont la réalisation des contrôles aux frontières tels que définis par le règlement (UE) 2016/399, ainsi que les règlements européens qui seront mis en œuvre dans les années à venir (Règlement (UE) 2017/2226) et l'amélioration et la facilitation des contrôles aux frontières pour les voyageurs aériens, maritimes, ferroviaires ou terrestres. Selon les applications et le type de finalité du traitement, est appliqué soit le règlement n° 2016/679 du 27 avril 2016 (RGPD) soit la directive n° 2016/680 du 27 avril 2016, dite directive « Police-Justice ». En effet, si une application est considérée comme concourant majoritairement à la finalité de facilitation des contrôles aux frontières, celle-ci sera encadrée par le RGPD alors que si l'application est considérée comme concourant à la finalité de réalisation de contrôles aux frontières, la directive Police-Justice sera appliquée.

Les données à caractère personnel collectées sont des données d'état civil issues du document de voyage, à savoir :

- Nom ;
- Prénoms ;
- Date de naissance ;
- Nationalité ;
- Sexe ;
- Image faciale contenue dans la puce.

Les données biométriques (empreintes digitales et image faciale), des données documentaires : le numéro, le type, la nationalité, le pays metteur du document de voyage, l'année d'expiration du document de voyage.

Les catégories de personnes concernées sont les personnes contrôlées aux frontières utilisant le dispositif kiosque de pré-enregistrement.

Pour l'exécution du service objet du présent contrat, le responsable de traitement met à la disposition du sous-traitant la documentation nécessaire au respect des présentes clauses, en particulier la politique de sécurité des systèmes d'information (PSSI) du Ministère de l'Intérieur et tout élément décrivant et encadrant les traitements.

ARTICLE 2. SECURITE

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 ;
- l'enregistrement des données de façon sécurisée afin de garantir leur confidentialité ;
- 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.

ARTICLE 3. OBLIGATIONS DU SOUS-TRAITANT VIS-A-VIS DU RESPONSABLE DE TRAITEMENT

Le sous-traitant doit être en conformité avec l'article 28 du RGPD :

3.1. Traitement des données

Le sous-traitant s'engage à traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/ont l'objet de la sous-traitance.

De même, il s'engage 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 Etats 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.

Par ailleurs, le sous-traitant doit garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent accord-cadre. Il veille 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.

S'agissant de ses outils, produits, applications ou services, le sous-traitant s'assure, par ailleurs, que soient pris en compte les principes de **protection des données dès la conception** et de **protection des données par défaut**.

3.2. 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.

3.3. 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).

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.

3.4. 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.

3.5. 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.

3.6. 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 ;
- Renvoyer toutes les données à caractère personnel au responsable de traitement ;
- 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.

3.7. 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.

3.8. 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 RGPD, 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 :
 - 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.

3.9. 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.

ARTICLE 4. OBLIGATIONS DU RESPONSABLE DE TRAITEMENT VIS-A-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.