I. Obligations du Titulaire concernant la sécurité de l'information

Le Titulaire s'engage à mettre en œuvre les mesures techniques et organisationnelles afin de se conformer à la politique de cybersécurité du groupe RATP et répondre spécifiquement aux exigences suivantes :

1. Formation

Le Titulaire s'engage à former et sensibiliser le personnel du marché à la cybersécurité, traiter le personnel non permanent avec les mêmes exigences.

2. Audit

Le Titulaire autorise le groupe RATP à exercer son droit d'audit et de contrôle sans accord préalable à distance dès lors que les tests et sondes utilisés par la RATP ou par des prestataires agissant pour son compte respectent les conventions techniques d'usage.

3. Gestion des incidents

Le Titulaire s'engage à mettre en œuvre une organisation pour répondre et réagir aux signalements de sécurité ; en particulier, un point de contact, un canal de communication et l'engagement de réalisation de plans de correction. Alerter en cas d'incident la RATP à l'adresse cybersecurite-groupe-ratp@ratp.fr .

4. Mesures de sécurité

Le Titulaire s'engage à respecter l'état de l'art en vigueur pour :

- les Services de messageries : utiliser des services d'échanges où l'authenticité des émetteurs et l'intégrité du message sont garanties ; en particulier, utiliser des services de courriels du domaine de l'entreprise Titulaire, ne pas utiliser d'adresses génériques.
- la Gestion des terminaux connectés : dispositifs de mise à jour de sécurité, dispositifs de lutte contre les logiciels malveillants, contrôle d'accès et authentification, limitations d'exposition sur les réseaux en limitant les ports à ceux utilisés et à l'utilisation de protocoles réputés sûrs.

5. Stockage des données

Le Titulaire s'engage à décrire la maitrise des enregistrements des données et transmission des données échangés au sujet du marché en cours. En particulier, la description des flux, les localisations des serveurs hébergeant les données.

6. Confidentialité des données

Le Titulaire s'engage à traiter les informations sensibles, à évaluer la criticité des données échangées à l 'exécution de la commande, signer et respecter les accords de confidentialité ou de non-divulgation si besoin, à protéger les données conservées et à supprimer les données à la fin du marché (ou à la fin de conservation réglementaire le cas échéant).

7. Gestion des sous-traitants

Le Titulaire s'engage à appliquer ces présentes exigences aux sous-traitants et à les contrôler ; à tenir à disposition les enregistrements des audits.

8. Evolution

Face à une situation majeure (évolutions des risques ou d'organisation) ou à un changement des mesures réglementaires, le Titulaire est tenu de faire évoluer sa politique de sécurité en fonction de ces évolutions.

II. Obligations du Titulaire en cas de Traitements de données à caractère personnel

Si le Titulaire, dans le cadre de la prestation effectuée, a accès ou traite des données à caractère personnel pour le compte de la RATP, alors il revêt la qualité de sous-traitant au sens de la règlementation 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 (ci-après, « ***le RGPD)***.

1. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte de la RATP, Responsable de traitement, les opérations de traitement de données à caractère personnel dans le cadre de la prestation.

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter leurs obligations issues de cette réglementation.

2. Description du traitement faisant l'objet de sous-traitance

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires à la fourniture de la prestation, objet du bon de commande qui lui a été passé.

3. Durée du traitement

La durée du traitement correspond à la durée indiquée sur le bon de commande, à compter de sa signature et pendant toute la durée de la prestation effectuée pour le compte du Responsable de traitement.

4. Obligations du sous-traitant vis-à-vis du responsable de traitement

Le Titulaire en tant que sous-traitant au sens RGPD s'engage à :

4.1. informer ses personnels salariés et ceux de ses sous-traitants que la RATP est susceptible de collecter et traiter dans ses systèmes informatiques des données à caractère personnel les concernant, dans le cadre de la gestion de ses dossiers. Ces traitements sont limités au seul usage de la RATP et leurs fichiers ne sont communiqués à aucun tiers non autorisé.

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

4.3. traiter les données conformément aux instructions documentées du Responsable de traitement (Bon de commande, Cahier des charges…). Si le sous-traitant considère qu'une instruction constitue une violation du RGPD 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 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.

4.4. garantir la confidentialité des données à caractère personnel traitées dans le cadre des présentes conditions générales.

4.5. veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu des présentes conditions générales :

- 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

4.6. 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

5. Sous-traitance ultérieure

Le Titulaire **communique la liste de ses propres sous-traitants** (ci-après, « ***les sous-traitants ultérieurs*** ») qui interviennent dans le cadre de la prestation effectuée pour le compte du Responsable de traitement, ou indique l'endroit où cette liste est rendue disponible.

Le sous-traitant peut faire appel à un autre sous-traitant pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Indépendamment de la mise en œuvre et du respect des obligations du Titulaire relative à la sous-traitance au sens de la loi de 1976, cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance et le délai à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant ultérieur doit être tenu de respecter les obligations des présentes conditions générales pour le compte et selon les instructions du Responsable de traitement. Il appartient donc 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. 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.

Si dans le cadre de la sous-traitance ultérieure, un transfert de données vers un pays tiers, le sous-traitant et le sous-traitant ultérieur doivent garantir le respect du chapitre V du RGPD en ayant recours aux Règles d'entreprise contraignantes conformément à l'article 47 du RGPD ou aux Clauses contractuelles types adoptées par la Commission Européenne sur la base de l'article 46§2 du RGPD, pour autant que les conditions d'utilisation de ces clauses contractuelles soient remplies. Le sous-traitant informe le responsable de traitement des garanties prises.

6. Droit d'information des personnes concernées

Si le titulaire réalise la collecte au titre de la présente commande, il doit, au moment de la collecte des données, fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de données qu'il réalise. La formulation et le format de l'information doivent être convenus avec la RATP avant la collecte de données.

7. 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 à l'adresse *protection-donnees@ratp.fr*

8. 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 heures après en avoir pris connaissance par courrier électronique à l'interlocuteur en charge du SI à la RATP ainsi qu'aux adresses suivantes : *cybersecurite-groupe-ratp@ratp.fr* et *protection-donnees@ratp.fr*. 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.

9. 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 et pour les éventuelles consultations préalables de l'autorité de contrôle.

10. Mesures de sécurité

Le sous-traitant s'engage à mettre en œuvre les mesures techniques et organisationnelles, adaptées à la sensibilité des données traitées, permettant de garantir leur confidentialité et leur sécurité. Ces mesures répondent a minima aux exigences listées en *Section 1 'Obligations concernant la sécurité de l'information'*. Il **communique au responsable de traitement la liste de ces mesures**, dès le démarrage de la prestation.

11. Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage, selon ce qui aura été convenu entre les parties, à détruire toutes les données à caractère personnel ou à les renvoyer au 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. 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 RGPD.

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 les informations requises à l'article 30§2 du RGPD.

14. Documentation

Le sous-traitant met à la disposition du Responsable de traitement 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.

15. Obligations du responsable de traitement vis-à-vis du sous-traitant

Le Responsable de traitement s'engage à :

15.1. fournir au sous-traitant les données nécessaires pour la fourniture de la prestation

15.2. documenter par écrit toute instruction concernant le traitement des données par le sous-traitant

15.3. veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le RGPD de la part du sous-traitant

15. 4. superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant