ANNEXE 5 : PROTECTION DES DONNEES PERSONNELLES

La présente Annexe a pour but de préciser les conditions dans lesquelles les Parties traitent les Données à caractère personnel dans le cadre du Contrat.

Le terme « Données à caractère personnel » désigne toute donnée relative à une personne physique identifiée ou identifiable directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification ou un identifiant en ligne ou à un ou plusieurs éléments spécifiques propres à son identité.

1. Traitements de Données à caractère personnel par La Poste

Dès lors que la prestation implique un traitement de Données à caractère personnel pour le compte du Client, il est convenu que La Poste aura la qualité de sous-traitant intervenant dans le cadre de la mise en œuvre du traitement pour le compte du Client.

Dans ce contexte, La Poste assure qu'elle dispose des compétences techniques et organisationnelles nécessaires afin de réaliser les prestations qui lui sont confiées par le Client dans le respect des obligations fixées dans le présent article et exclusivement pour l'objet prévu au Contrat.
En conséquence, La Poste s'engage à :

- ne procéder au traitement de Données à caractère personnel que sur instruction écrite du Client et informer ce dernier si une instruction lui paraît contraire à la règlementation sur la protection des données ;
- ne conserver les Données à caractère personnel traitées, sous une forme permettant l'identification des personnes, que le temps nécessaire à l'exécution des Prestations (13 mois après la livraison pour les colis nationaux pour le traitement des réclamations, 4 ans pour les colis DOM et Hors Union Européenne pour des raisons fiscales) ;
- accompagner le Client dans le cadre de la réalisation d'études d'impact sur la vie privée ;
- aider le Client, sous réserve d'en être informé, dans toute la mesure du possible, afin de répondre à toute demande d'exercice de droits par les personnes concernées et/ou toute demande d'information des autorités de contrôle et de protection des données ;
- informer le Client de toute demande relative aux Données à caractère personnel qui lui serait adressée directement, dans le cas où la demande concerne les Données à caractère personnel transmises par le Client

Le Client s'engage à respecter l'ensemble de la réglementation applicable en matière de protection des Données à caractère personnel, notamment en ce qui concerne l'information des personnes dans le cadre de la transmission de leurs Données à caractère personnel au Prestataire pour les besoins de l'exécution du présent Contrat.

2. Sécurité et confidentialité des Données à caractère personnel

La Poste prendra toute mesure nécessaire pour préserver l'intégrité, la disponibilité et la confidentialité des Données à caractère personnel.
La Poste s'engage notamment à mettre en place les mesures techniques et organisationnelles permettant d'assurer un niveau de sécurité conformes à l'état de l'art.
La Poste s'engage en particulier à :

- mettre en œuvre les mesures nécessaires afin de protéger les Données à caractère personnel contre une destruction fortuite ou illicite, une perte accidentelle, une altération, une divulgation ou un accès non autorisé ;
- ne rendre accessibles et consultables les Données à caractère personnel traitées qu'aux seuls personnels dûment habilités en raison de leurs fonctions et qualité, dans la stricte limite de ce qui leur est nécessaire à l'accomplissement de leurs fonctions ;
- notifier au Client, sous 48 heures à partir du moment où il en a connaissance, toute violation de Données à caractère personnel.
- Dans ce contexte La Poste communiquera au Client tous les éléments dont il dispose concernant les conditions entourant cette violation de Données à caractère personnel et notamment la nature et l'étendue des Données à caractère personnel impactées, le nombre de personnes concernées, les conséquences probables et les conditions techniques dans lesquelles la violation a eu lieu.

La Poste dispose d'une Politique de Sécurité des Systèmes d'Information (PSSI) qui s'appuie sur le standard ISO 27002 et porte sur l'ensemble des SI en tant qu'actifs et en tant que ressources support des activités. Les règles de sécurité techniques et organisationnelles couvrent les technologies, les applications Métiers, les données manipulées par les SI, la téléphonie sous IP, les installations, les intervenants sur les ressources du SI etc. Les mesures de sécurité de la PSSI englobent notamment (liste non exhaustive) :

- La sécurité logique (durcissement des environnements, cloisonnement des architectures réseau et filtrage, contrôle d'accès par authentification, politique de mots de passe, protection par logiciel antimalware …)
- La gestion des traces et des preuves
- La gestion des correctifs de sécurité
- La classification des actifs SI
- La gestion des tiers
- La sécurité des applications et des flux
- La gestion des incidents de sécurité
- Etc.

La PSSI est accompagnée d'une Charte annexée au règlement Intérieur portant sur les conditions de sécurité dans lesquelles les collaborateurs doivent utiliser les outils informatiques mis à leur disposition et d'une Charte dédiée aux fonctions informatiques et techniques.

La PSSI s'appuie sur une filière qui regroupe l'ensemble des fonctions tournées vers la sécurité des SI, localisées au sein des différentes entités. Chaque Branche, BU et filiale dispose notamment d'un Responsable Sécurité du SI (RSSI).

La Poste s'est doté d'une Direction dédiée à la lutte contre la Cybercriminalité dont la mission est de mettre en œuvre des systèmes de protection et de surveillance informatique. Des audits de sécurité internes et externes par des sociétés qualifiées PASSI par l'ANSSI sont régulièrement effectués.

3 - Communication à des tiers

Les Données à caractère personnel traitées en exécution du Contrat ne pourront faire l'objet d'aucune divulgation à des tiers en dehors des cas prévus dans le Contrat ou de ceux prévus par une disposition légale et/ou réglementaire.
La Poste informera le Client de toute demande d'accès ou de communication émanant d'un tiers se prévalant d'une autorisation découlant de l'application de dispositions légales ou réglementaires.

4 –Documentation

La Poste fera son affaire de la bonne tenue de son registre des traitements de Données à caractère personnel en veillant à y inscrire le(s) traitement(s) qu'il met en œuvre pour le compte du Client.

Par ailleurs, La Poste s'engage à tenir un registre et un process documenté de notification en cas de Violations de Données. La Poste documentera toutes les informations pertinentes concernant les circonstances de la Violation de Données, les conséquences et les mesures correctives prises pour en atténuer les éventuelles conséquences négatives.

5 -Transferts de Données à caractère personnel
5.1 Sous-traitants

Le responsable de traitement donne une autorisation générale au Prestataire lui permettant de recourir à d'autres sous-traitants dans le cadre de l'exécution de ses prestations. A ce titre, La Poste s'engage à mettre à la charge de son (ou ses) sous-traitant(s) les mêmes obligations que celles fixées au présent Contrat pour que soient respectées la confidentialité, la sécurité et l'intégrité des Données à caractère personnel. Sur simple demande, La Poste communiquera au responsable de traitement l'identité des sous-traitants devant accéder, stocker, ou intervenir sur les Données Personnelles informatisées ou non.

Pour les sous-traitants ayant accès aux Données à Caractère Personnel non informatisées sans les « processer » au sens du Règlement Européen (exemple : consultation des bordereaux de livraison), y compris au sein de son groupe, La Poste s'engage à imposer contractuellement à ses propres sous-traitants les mêmes obligations en matière de protection de Données que celles fixées au présent Contrat, en particulier pour ce qui est de présenter 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 de la Loi de 1978 et du Règlement Européen.

5.2 Transfert hors Union Européenne

Dans l'hypothèse où La Poste réaliserait tout ou partie du traitement de Données à caractère personnel en dehors du territoire d'un pays membre de l'Union européenne, de l'Espace Economique Européen (EEE) ou d'un pays reconnu comme adéquat par l'Union Européenne – y compris l'hébergement – il s'engage à encadrer le transfert des Données à caractère personnel par des garanties appropriées, notamment des clauses types adoptées par la Commission Européenne.
Dans le cadre de l'externalisation d'une partie des activités du Service Clients de La Poste ainsi que pour la réalisation de la tierce maintenance applicative d'application(s) informatique(s), les données font l'objet d'un transfert au Maroc. Ce transfert intervient dans le respect des conditions et garanties adaptées à assurer la protection des Données à caractère personnel transmises par le Client à La Poste dans le cadre de ce contrat, notamment par la signature de clauses contractuelles types selon les modalités prévues par décision de la Commission Européenne, pour le transfert de Données à caractère personnel vers des sous-traitants établis dans des pays tiers.

6 – Effacement des Données à caractère personnel
Au terme du Contrat et dans le respect des délais de prescription postale, La Poste s'engage à effacer, selon les instructions et dans les délais indiqués par le Client, l'ensemble des Données à caractère personnel traitées. L'effacement pourra, à la demande du Client, être attesté par le Prestataire. .

7 – Audit

Le Client, s'il le souhaite, pourra réaliser, à ses frais, un audit, directement ou par l'intermédiaire de tout sous-traitant externe indépendant, non concurrent direct du Prestataire, afin de s'assurer du respect des obligations du Prestataire.
Il est convenu entre les Parties que le Client ne pourra réaliser un audit qu'une fois par an et devra procéder à un tel audit durant les heures d'ouverture, sans toutefois que l'audit ne puisse perturber les activités du Prestataire. Dans ce cas, le Client communiquera au Prestataire au moins un mois avant toute demande d'audit, la date et le périmètre de l'audit ainsi que le nom et les références des personnes en charge de l'audit. Le Client s'engage à prendre toutes les précautions afin de s'assurer que l'audit ne porte pas atteinte au système d'information de La Poste.

Toutefois, sauf en cas de manquement avéré et justifié, La Poste pourra produire le résultat d'un audit précédent réalisé par un tiers sur le même périmètre et datant de moins de 12 mois en lieu et place de l'audit demandé par le Client. Dans ce cas, La Poste sera réputé avoir satisfait le droit d'audit du Client.
La Poste pourra refuser pour motif légitime les personnes désignées pour réaliser l'audit. En cas de refus, les Parties se rencontreront afin de s'accorder sur la désignation de l'auditeur. Tout différend sera porté devant les juridictions compétentes.
La Poste collaborera de bonne foi avec l'auditeur et lui communiquera toutes informations, documents ou explications nécessaires à la réalisation de l'audit et lui permettra d'accéder à tous sites, installations informatiques, outils et moyens du Prestataire utilisés pour rendre les prestations.

Un rapport de l'audit sera envoyé à La Poste.

8- Exercice des droits

Conformément à la réglementation en vigueur en matière de protections des données personnelles le Client dispose à tout moment d'un droit d'accès, de rectification, d'opposition de limitation du traitement, de portabilité et d'effacement dans les conditions prévues par les textes.
Pour exercer ces droits, le Client peut envoyer un courrier à :
La Poste - BP 10245 - 33506 Libourne Cedex
ou bien un mail à l'adresse : mesdonneespersonnelles.laposte@laposte.fr

9- Délégué à la Protection des Données

La Poste dispose d'un Délégué à la Protection des données, dont les coordonnées sont les suivantes :
Madame la Déléguée à la Protection des Données –
CP C703 –
9 rue du Colonel Pierre Avia –
75015 PARIS