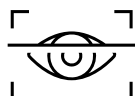


En bref



Nous traitons vos données dans le cadre de notre relation contractuelle uniquement



Vous n'avez le droit d'accéder qu'aux données strictement nécessaires à la tâche que nous vous avons confiée



Vous êtes garant de la sécurité des données que nous vous confions



Vous avez l'obligation d'échanger les données de façon sécurisée, chiffrée



Vous avez l'interdiction de réexploiter les données pour votre propre compte sauf avec nos accord préalable

1. Préambule

Dans le cadre de sa gestion administrative et de ses relations avec ses fournisseurs, prestataires et partenaires, l'APST37, responsable de traitement, est amené à collecter et traiter des données à caractère personnel sur les salariés, dirigeants ou représentants de ses fournisseurs, prestataires et partenaires.

Par ailleurs la protection des données à caractère personnel est l'une des préoccupations majeures de l'APST37. A travers ce document l'APST37 renouvelle son engagement à assurer la protection, la confidentialité et la sécurité des données à caractère personnel qu'il traite.

La présente Charte répond alors à un double objectif :

- D'une part, informer en toute transparence les personnes concernées auprès de nos fournisseurs, prestataires et partenaires de la manière dont leurs données sont traitées par l'APST37 ;
- D'autre part, de rappeler aux fournisseurs, prestataires, et partenaires qui pourraient être amenés à manipuler des données à caractère personnel dans le cadre de l'exécution du contrat qui les lie avec l'APST37, leurs obligations en matière de protection des données.

Cette Charte s'adressant aux personnes employées par les fournisseurs, prestataires et partenaires de L'APST37, il appartient aux organismes de communiquer le présent document à leurs préposés.

2. Champ d'application

La présente Charte s'applique à l'ensemble des fournisseurs, partenaires et prestataires de LIAPST37 (ci-après dénommés « **Tiers** ».)

3. Définitions

Règlement Général relatif à la Protection des Données (RGPD) : réglementation applicable aux organismes privés et publics traitant des données à caractère personnel.

Données à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable (dénommée « personne concernée ») (exemple nom, prénom, adresse mail, numéro de téléphone, numéro de dossier, etc.)

Délégué à la protection des données (DPD ou DPO) : personne chargée d'assurer la protection des données à caractère personnel. Vous pouvez, si besoin est, la contacter à l'adresse mail suivante : dpo@apst37.fr

Responsable de traitement : sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, il s'agit de la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Sous-traitant : il s'agit de la personne physique ou morale, autorité publique, service ou autre organisme qui traite des données à caractère personnel pour le compte du responsable de traitement.

4. Informations relatives aux salariés, dirigeants et représentants des Tiers

L'APST37 informe les Tiers qu'il est amené à traiter les données à caractère personnel de contact des salariés, dirigeants ou représentants de ces derniers à savoir :

- Civilité, nom, prénom ;
- Coordonnées professionnelles (numéros de téléphone fixe et mobile, adresse postale si nécessaire, adresse électronique) ;
- Titre et fonctions professionnelles voire historique professionnel détaillé dans le cadre de projets spécifiques (par exemple si votre CV nous a été présenté en vue de vous retenir sur le projet) ;
- Données collectées pour gestion des contrôles d'accès de zones soumises à restriction (ex : historique de badge, registre des visiteurs) ;
- Données nécessaires au contrôle et à l'évaluation de la qualité des prestations réalisées par nos Tiers.

Ces informations sont collectées directement auprès des personnes concernées ou, par exception, transmises par l'employeur des personnes concernées lors de l'entrée en relation ou ultérieurement. Elles font l'objet d'un traitement pour les finalités suivantes :

- Gestion administrative des Tiers dont la gestion des commandes et la facturation ;
- Gestion des relations commerciale et contractuelle avec les Tiers ;
- Gestion de la comptabilité générale de l'APST37 ;
- Gestion de la sécurité des locaux et installations de l'APST37 ;
- Contrôle et évaluation de la qualité des prestations réalisées par les Tiers.

L'APST37 conserve les données à caractère personnel des salariés, dirigeants ou représentants des Tiers pendant la durée nécessaire à l'accomplissement des missions ci-dessus évoquées et, au-delà, pour la durée nécessaire à l'exercice de toute action judiciaire susceptible d'être engagée entre les parties. Sauf exception les données sont ainsi conservées pendant la durée de la relation contractuelle entre L'APST37 et les organismes Tiers, augmentée de 5 ans (prescription de droit commun).

Ces données sont traitées par les services gestionnaires de l'APST37, ses sous-traitants et des organismes habilités par la loi telle que l'administration fiscale.

Chaque salarié, dirigeant ou représentant dont les données sont traitées dispose de droits sur ses données : droit d'accès, de rectification, d'opposition et d'effacement. Les personnes concernées peuvent exercer leurs droits en s'adressant au Délégué à la Protection des Données (ou « DPO ») de l'APST37, à l'adresse mail suivante : dpo@apst37.fr

Chaque personne concernée dispose enfin du droit d'introduire une réclamation auprès d'une autorité de contrôle relativement aux traitements de données mis en œuvre tel qu'indiqué précédemment ainsi qu'à l'exercice de ses droits s'y rattachant. En France, il s'agit de la CNIL.

Il appartient aux Tiers d'informer chacun de ses salariés, dirigeants ou représentants des droits offerts par l'APST37 au titre du RGPD.

5. Engagements des Tiers en matière de protection des données à caractère personnel

5.1 Traitements réalisés par les Tiers pour leur propre compte

Si les Tiers mettent en œuvre des traitements de données à caractère personnel pour leur propre compte, à partir de données transmises par l'APST37 ou non, il est expressément entendu qu'ils en assument seuls les obligations et responsabilités en matière de traitement de données résultant des dispositions du RGPD et de toute autre réglementation afférente actuelle ou future.

5.2 Traitements réalisés par les Tiers pour le compte de l'APST37

Pour les besoins de l'exécution de leurs prestations contractuelles pour l'APST37, les Tiers peuvent se voir communiquer des données à caractère personnel dont l'APST37 est le responsable de traitement.

Dès lors, chaque Tiers s'engage à traiter les données à caractère personnel auxquelles il a accès dans le respect de la réglementation applicable en matière de protection des données et notamment s'engage à :

- Traiter les données transmises par l'APST37 pour la ou les seules finalités faisant l'objet de leur contrat avec l'APST37 et conformément aux instructions données par ce dernier ;
- Garantir la sécurité des données en mettant en œuvre les mesures techniques et organisationnelles nécessaires ;
- Ne pas communiquer les données transmises à un tiers sans autorisation préalable de l'APST37 ;
- Notifier à l'APST37 de tout incident de sécurité ou violation de données à caractère personnel dans un délai maximum de 24 heures après en avoir pris connaissance ;
- Détruire les données transmises par l'APST37 au terme du contrat ou marché selon les cas.

Par ailleurs, pour les Tiers agissant en qualité de sous-traitant au sens du RGPD dont les hébergeurs, prestataires d'infogérance, etc., ces derniers s'engagent à mettre en place avec l'APST37 les clauses obligatoires de l'article 28 du RGPD.

5.3 Sécurité et échanges des données

L'APST37 et chacun de ses Tiers s'engagent à mettre en œuvre les mesures de sécurité organisationnelles et techniques appropriées, notamment :

- Utiliser des outils de partage et de stockage de données respectant les recommandations de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et de la CNIL en la matière. Il est rappelé à ce titre qu'il est interdit de :
 - Transmettre des données à caractère personnel en clair dans un email. La transmission de données par email ne doit être utilisée qu'en dernier recours. Le cas échéant la mise en place de mesures de sécurité complémentaires est indispensable, par exemple le placement des données dans une archive chiffrée jointe à l'email en parallèle de la communication de la clé de chiffrement par un autre canal (téléphone par exemple). A cet égard, une tolérance est accordée lorsque l'échange de données par un email concerne un faible volume de données ayant une criticité minimal tel qu'un nom un prénom, ou encore la fonction d'une personne. Ceci étant, si le volume de données échangées est important (ex : un listing de personne avec le nom et prénom) ou que les données sont qualifiées de sensibles au sens du RGPD ou de la loi informatique et libertés (ex : données de santé, données financières etc.), ces données doivent être échangées de façon sécurisée (Ex : FTP dédié, chiffrement de la pièce jointe...)
 - Transmettre des données à caractère personnel via des outils du marché engendrant des transferts de données à caractère personnel hors Union européenne, sauf à avoir obtenu l'accord préalable de l'APST37;
 - Transmettre des données à caractère personnel des outils du marché avec hébergement externalisé (SaaS) sans avoir analysé minutieusement au préalable la sécurité et la localisation des données ;
- Eviter d'utiliser des périphériques mobiles pour le stockage des données sans que des mesures de sécurité complémentaires tel que le chiffrement soient mises en place.

5.4 Engagement de confidentialité

L'APST37 et chacun de ses Tiers s'engagent à préserver la confidentialité de toutes les données et informations confidentielles émanant de l'une ou l'autre des parties et à ne pas les divulguer sans autorisation préalable de l'autre.

Les « informations confidentielles » recouvrent toutes informations ou données communiquées par les parties que ces informations aient été délivrées par écrit, oralement ou par tout autre moyen.

Il appartient particulièrement à chacun de :

- Ne pas partager d'informations concernant des clients à une personne n'ayant pas strictement besoin d'en connaître, y compris en interne ou auprès d'autres clients du même groupe ;
- Ne pas partager d'informations à des organismes tiers sans avoir demandé l'accord de l'APST37 au préalable et sans s'être assuré de la légitimité de ces organismes ;
- Avoir un comportement de nature à conserver la confidentialité des informations détenues à tout moment, notamment en s'assurant de la confidentialité des supports et lieux dans lesquels des informations sont échangées (notamment, ne pas échanger oralement d'informations dans des lieux publics où dans lesquels vous pouvez facilement être entendu).