Charte RGPD de la Pharmacie du Viaduc
Protection des données personnelles

PREAMBULE :

La présente charte engage la pharmacie du Viaduc), à respecter les règlementations sur la protection des données personnelles, notamment celle du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 dit le Règlement Général sur la Protection des Données (RGPD).

La charte est, de fait, annexée au contrat en cours et au futurs contrats passés avec les clients désignés comme Responsable de traitement. La Pharmacie du Viaduc est désignée comme Sous-Traitant au sens RGPD.

I. Objet de l'engagement

Le but de la charte est d'offrir aux clients de la Pharmacie du Viaduc qui utilise ses prestations les garanties adéquates concernant la protection des données à caractère personnel.

La charte présente sous forme de clauses les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement (par exemples Pharmacies clientes) les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles, les Parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le Règlement Général sur la Protection des Données.

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

Les caractéristiques des traitements de données personnelles effectuées par le Sous-traitant pour le compte du Responsable de Traitement sont détaillées en annexe 1. Toute modification de l'annexe 1 devra donner lieu à l'établissement d'un avenant signé par les Parties.

III. Durée de l'engagement

Les présentes clauses entrent en vigueur à compter de la date de démarrage de la prestation et pour la durée du contrat avec le Responsable de traitement.

IV. 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. (Voir annexe 1).

2. 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.

3. Garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat.

4. Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent contrat :
- 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. Sous-traitance :

6.1 - Le sous-traitant peut faire appel à des sous-traitant ultérieurs, ceux-ci sont indiqués dans l'annexe 2 de la charte. Si pour mener des activités de traitement spécifiques le sous-traitant a besoin de faire appel à un autre sous-traitant ultérieur, il informe préalablement et par écrit le responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. 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. Le responsable de traitement dispose d'un délai minium de 15 jours 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. En cas de recrutement d'autres sous-traitants ultérieurs, le sous-traitant doit recueillir l'autorisation écrite, préalable et spécifique du responsable de traitement.

6.2 - Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat 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 que le traitement réponde aux exigences du règlement européen sur la protection des données. 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.

Les informations sur les éventuels sous-traitants ultérieurs se trouvent dans l'annexe 2.

7. Droit d'information des personne 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

8. 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).

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 et en tout état de cause dans les 72 h au plus tard après en avoir pris connaissance. 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.

La notification contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Après accord du responsable de traitement, le sous-traitant communique, au nom et pour le compte du responsable de traitement, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque

élevé pour les droits et libertés d'une personne physique.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

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. Mesures de sécurité

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité suivantes qui garantissant un niveau de sécurité adapté au risque (Voir Annexe 2).

12. Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage à détruire toutes les données à caractère personnel ou à renvoyer toutes les données à caractère personnel au responsable de traitement. Le renvoi s'accompagne 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 (procès-verbal).

13. 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. Le responsable de traitement communique au sous-traitant les coordonnées de son délégué à la protection des données (dpo@viaducpharma.com).

14. 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.

5. 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.

La durée de l'audit ne devra pas excéder 1 jour ouvré, ni faire peser sur la Pharmacie du Vieux

Port une charge supérieure à un (1) jour-homme. Il est convenu entre les Parties que la Pharmacie du Vieux Port ne communiquera les informations ou ne fournira des accès à tout Tiers Auditeur que pour le périmètre qui concerne les Données à Caractère Personnel du Client. L'assistance apportée par le personnel de la pharmacie dans le cadre de tout audit fera l'objet d'une facturation au temps passé au tarif en vigueur au moment de l'audit. Le Client s'engage à transmettre, gratuitement, les conclusions du rapport d'audit à la Pharmacie du Viaduc, et ce dès la première demande.

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

Le responsable de traitement s'engage à :

- fournir au sous-traitant les données visées au chapitre II des présentes clauses
- 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 européen sur la protection des données, notamment à ne confier des données personnelles qui respectent les obligations RGPD (légalité du traitement, information des personnes, voire obtention du consentement).

Charte RGPD ANNEXE 1 : 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 fournir le ou les service(s) indiquées dans nos contrats en cours.

La nature des opérations réalisées sur les données est l'utilisation de données dans le but de réaliser les opérations liées à la fourniture de nos prestations.

La ou les finalité(s) du traitement sont :
- La gestion des commandes de l'activité Préparatoire de la pharmacie du Viaduc.
- L'hébergement des données y compris des données de santé de type ordonnance des clients/patients des responsables de traitement,
- La supervision et le maintien en condition opérationnelles des solutions,
- Le sort des données (transmission et/ou suppression des données)

Les données à caractère personnel traitées sont :
- Les données courantes d'identification et de contact des clients: nom, prénom, adresse, numéro de téléphone, adresse électronique ;
- Toutes les données transmises par le client dans le cadre de notre service préparatoire :
    - données d'identification,
    - information particulières (type allergies),
    - données de santé (ordonnance) ;
- Toutes les données de sauvegarde.

Les catégories de personnes concernées sont :
- Les collaborateurs des parties prenantes
- Les personnes figurant dans les commandes préparatoires.

Pour l'exécution du service objet du présent contrat, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires suivantes :

- Information sur ses représentants,
- Coordonnées de son délégué à la protection des données ou interlocuteur RGPD.

Charte RGPD ANNEXE 2 : Description des mesures de protection de la pharmacie du Viaduc

1. Désignation d'un référent à la protection des données

La pharmacie du Viaduc s'est dotée d'un DPO (DataProtection Officer)
Les coordonnées du DPO sont :
Chloé PEILLEX
Adresse postale : 41 rue Antoine EYRAUD 42410
PELUSSIN
Courriel: dpo@viaducpharma.com

2. Sécurité Physique

   Il y a contrôle des accès physiques pour l'accès au bâtiment. L'accès est interdit au public. Tout visiteur est systématiquement accompagné. Pour les documents sensibles, les bureaux sont fermés à clés.

3. Contrôle d'accès logique

   L'accès au système d'information exige une identification et une authentification préalable. Tout utilisateur, interne ou externe, est identifié de façon unique avec une gestion des arrivées, absences et départs. L'authentification est effectuée sur la base d'un login et d'un mot de passe dont la complexité correspond à l'état de l'art. L'identifiant et le mot de passe sont strictement confidentiels et personnels, l'utilisateur ne doit donc pas les communiquer à un tiers, ni s'authentifier pour laisser un tiers utiliser ses droits.

   Le Système d'Information est protégé vis-à-vis de l'extérieur à l'aide de filtres d'accès appliqués sur les équipements en tête de son réseau (firewall). Au niveau des applicatifs métiers, chaque utilisateur possède un droit d'accès en fonction de son rôle dans l'organisation, permettant de limiter au juste nécessaire l'accès aux données concernées.

   Les applications critiques contenant des informations métiers sensibles sont protégées par des mesures de sécurité pour authentifier nominativement les utilisateurs et enregistrer leurs connexions. Des mécanismes de renouvellement de mot de passe et de déconnexion automatique après un délai d'inactivité sont mis en œuvre.

4. Traçabilité

   Les accès à l'annuaire de sécurité, aux serveurs de fichiers, aux applications métiers critiques sont journalisés afin de détecter les tentatives d'intrusions.

5. Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

   Les serveurs et postes de travail sont protégés par un antivirus mis à jour régulièrement et de manière centralisée. Le maintien du niveau de sécurité (en particulier vérification d'absence de

risque lors de l'installation de nouveaux matériels ou logiciels ou de connexion de matériels mobiles...) doit faire l'objet de dispositions techniques sous la responsabilité du responsable informatique.

6. Sauvegarde des données

   L'entreprise dispose d'un plan de sauvegarde informatique qui concerne la sécurité de toutes données des clients.

7. Chiffrement des données / anonymisation

   L'accès aux plateformes et sites web est sécurisé par un protocole réseau chiffré TLS et un filtrage par un pare-feu.

8. Mécanisme de purge des données

   Suppression manuelle des données en fin de prestation.

9. Maitrise des sous-traitants ultérieurs

   Les contrats relatifs à des prestations informatiques (intégration de logiciels, maintenance et télémaintenance...) et d'hébergement comportent des clauses de confidentialité et de conformité au RGPD (règlement européen sur la protection des données à caractère personnel Loi du 25 mai 2018).

   Les sous-traitants ultérieurs d'ores et déjà acceptés par le Client pour les services d'hébergement de données sont :

Raison social	Localisation	Périmètre	Transfert hors Union UE
IDRIS SOFTWARE	France	Hébergeur de données	Non
LGPI	France	Hébergeur de données	Non

10. Sensibilisation du personnel

    Le personnel manipulant des données personnelles a été sensibilisé au RGPD et aux bonnes pratiques en matière de protection des données.