

Chaque partie s'engage à :

1. Traiter les données uniquement pour la seule finalité suivante : prise de rendez-vous avec le cabinet médical itinérant ;
2. Si l'une des parties considère qu'un échange de données 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 États membres relative à la protection des données, il en informe immédiatement l'autre partie ;
3. Garantir la confidentialité des données à caractère personnel traitées d. Cette obligation de confidentialité s'applique sans limitation de durée. À cet effet, les parties s'engagent à ne divulguer ces informations confidentielles qu'à leurs seuls personnels et, le cas échéant, prestataires (sous-traitants au sens du Rgpd) ayant à en connaître et notamment par la mise en œuvre de procédés d'authentification adaptés ;
4. Veiller à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité et 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. Garantir le droit d'information des personnes concernées : chaque partie, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de données réalisés ;
7. Répondre à l'exercice des droits des personnes<sup>1</sup> : Dans la mesure du possible, chaque partie doit s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : . Les parties collaborent entre elles, si nécessaire, pour apporter les réponses à ces demandes ;
8. Notifier les violations de données à caractère personnel : chaque partie :
  - \* est responsable des suites à donner après la détection d'une violation de données à caractère personnel dans le cadre du traitement qu'il exécute.
  - \* informe l'autre partie de la survenance de toute violation de données à caractère personnel susceptible d'avoir, directement ou indirectement, des conséquences pour l'autre partie, ainsi que de toute plainte qui lui serait adressée par une personne concernée par le traitement. Cette information intervient dans les plus brefs délais et, sauf mention contraire au sein d'une convention d'application, au plus tard 36 heures après la découverte de la violation de données ou la réception de la plainte. De plus, les parties se tiennent informées de toute difficulté ou anomalie détectée ;
9. Mettre en œuvre les mesures de sécurité permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement. Chaque partie s'engage à mettre en œuvre les mesures de sécurité techniques et organisationnelles appropriées afin de garantir le niveau de sécurité nécessaire à la protection des données. Si, pour l'exécution de la convention, les parties recourent à des prestataires (sous-traitants au sens du Rgpd), les contrats qu'elles concluent avec eux présentent, s'agissant des mesures de sécurité mises en œuvre, des garanties équivalentes à celles mises en place dans ce cadre.
10. Indiquer le nom de la personne en charge de la protection des données.
  - Département : Catherine Charpentier, Déléguée à la protection des données, (protectiondonnees@departement18.fr).
  - structure prenant le rendez-vous :
11. Chaque partie s'engage à effectuer, pour son propre compte, les opérations de conformité légales.

---

<sup>1</sup> droit d'information, d'accès, de rectification, d'opposition, d'effacement, droit à la limitation du traitement, de portabilité et de faire intervenir une personne dans le processus de décision sous réserve de l'application des mesures légales y faisant obstacle