



**ACCORD DE TRAITEMENT
DES DONNÉES À CARACTÈRE PERSONNEL (DPA)**

Article 28 du Règlement (UE) 2016/679 (RGPD)

Annexe aux conditions générales de vente et d'abonnement MediWay

Le présent Accord de traitement des données (ci-après le « DPA ») est annexé aux conditions générales de vente et d'abonnement (les « CGV ») et au Bulletin de Souscription conclus entre MediWay et le Transporteur (ensemble, le « Contrat »), dont il fait partie intégrante. Il a pour objet d'encadrer les traitements de données à caractère personnel, en particulier de données de santé, que MediWay réalise pour le compte du Transporteur au moyen de la Plateforme. Les termes commençant par une majuscule ont le sens qui leur est donné dans les conditions générales d'utilisation de la Plateforme (les « CGU ») et dans les CGV. En cas de contradiction entre le présent DPA et le Contrat s'agissant de la protection des données, le présent DPA prévaut.

ARTICLE 1 – QUALITÉ DES PARTIES :

Aux fins des traitements de données à caractère personnel réalisés au moyen de la Plateforme pour l'organisation et l'exécution des transports confiés au Transporteur :

- le Transporteur agit en qualité de responsable de traitement ; il détermine les finalités et les moyens des traitements portant sur les données des patients qu'il transporte, de ses Conducteurs et de son personnel ;
- MediWay agit en qualité de sous-traitant ; elle traite ces données pour le compte et sur instructions documentées du Transporteur, dans les conditions du présent DPA.

Il en va notamment ainsi des données relatives aux Missions affectées au Transporteur, à son planning, au dossier de transport dématérialisé (PMT, avis de passage) et aux PMT qu'il dépose au titre d'un Transport Externe, dans les conditions de l'article 8.3 des CGV.

Par exception, MediWay agit en qualité de responsable de traitement autonome pour ses traitements propres qui ne sont pas réalisés pour le compte du Transporteur, notamment la gestion des comptes utilisateurs et des habilitations, la sécurité et la traçabilité de la Plateforme, la relation contractuelle et la facturation, l'établissement de statistiques agrégées, l'amélioration de la Plateforme et la consultation, avec le consentement du Patient, de la situation de ses droits auprès de l'assurance maladie (article 12.8 des CGU). Ces traitements sont régis par la politique de confidentialité de MediWay et non par le présent DPA.

ARTICLE 2 – OBJET, DURÉE ET DESCRIPTION DES TRAITEMENTS :

Le présent DPA a pour objet de définir les conditions dans lesquelles MediWay s'engage à effectuer, pour le compte du Transporteur, les opérations de traitement de données à caractère personnel décrites ci-après. La nature, la finalité, les catégories de données et de personnes concernées ainsi que la durée des traitements sont précisées en Annexe 1.



Le présent DPA prend effet à la date de formation du Contrat, dans les conditions de l'article 5.3 des CGV, et demeure applicable pendant toute la durée des traitements réalisés pour le compte du Transporteur au moyen de la Plateforme.

ARTICLE 3 – INSTRUCTIONS DOCUMENTÉES :

MediWay traite les données à caractère personnel uniquement sur instructions documentées du Transporteur.

Le Contrat, le paramétrage de la Plateforme et l'utilisation qui en est faite par le Transporteur et les personnes agissant sous son autorité constituent les instructions initiales. MediWay informe immédiatement le Transporteur si, selon elle, une instruction constitue une violation du RGPD ou d'une autre disposition applicable en matière de protection des données.

ARTICLE 4 – OBLIGATIONS DE MEDIWAY (SOUS-TRAITANT) :

MediWay s'engage à :

- ne traiter les données que pour les seules finalités faisant l'objet de la sous-traitance et conformément aux instructions documentées du Transporteur ;
- garantir la confidentialité des données traitées, et veiller à ce que les personnes autorisées à les traiter s'engagent à en respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
- 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 (article 25 du RGPD) ;
- mettre en œuvre les mesures techniques et organisationnelles appropriées pour assurer la sécurité des données (article 32 du RGPD), telles que décrites en Annexe 2 ;
- héberger les données de santé auprès d'un hébergeur de données de santé (HDS) certifié conformément à l'article L.1111-8 du Code de la santé publique ;
- assister le Transporteur, compte tenu de la nature du traitement, dans l'exercice par les patients de leurs droits (accès, rectification, effacement, opposition, limitation, portabilité) ;
- aider le Transporteur à garantir le respect de ses obligations en matière de sécurité, de notification des violations, d'analyse d'impact (AIPD) et de consultation préalable de la CNIL ;
- mettre à la disposition du Transporteur toutes les informations nécessaires pour démontrer le respect des obligations de l'article 28 du RGPD et permettre la réalisation d'audits, dans les conditions de l'article 8 ;
- tenir un registre de toutes les catégories d'activités de traitement effectuées pour le compte du Transporteur, conformément à l'article 30.2 du RGPD ;
- au terme des traitements, et au choix du Transporteur, supprimer les données ou les lui restituer, puis détruire les copies existantes, sauf obligation légale de conservation, dans les conditions de l'article 14.9 des CGV et de l'Annexe 1.

ARTICLE 5 – SOUS-TRAITANCE ULTÉRIEURE :

Le Transporteur autorise de manière générale MediWay à recourir à des sous-traitants ultérieurs pour l'exécution des Services, notamment pour l'hébergement des données de santé, le stockage des fichiers, la lecture automatisée des PMT et l'envoi de notifications. La liste des sous-traitants ultérieurs en vigueur figure en Annexe 3.

MediWay informe le Transporteur de tout ajout ou remplacement d'un sous-traitant ultérieur, par écrit et au moins trente (30) jours à l'avance ; le Transporteur peut formuler des objections pendant ce délai. MediWay impose à chaque sous-traitant ultérieur, par contrat, les mêmes



obligations de protection des données que celles prévues au présent DPA, et demeure pleinement responsable envers le Transporteur de leur exécution.

ARTICLE 6 – SÉCURITÉ ET VIOLATION DE DONNÉES :

MediWay met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, en tenant compte notamment du caractère des données de santé (chiffrement, contrôle des accès, journalisation, sauvegardes, cloisonnement — voir Annexe 2).

En cas de violation avérée de données à caractère personnel, MediWay notifie le Transporteur dans les meilleurs délais et au plus tard quarante-huit (48) heures après en avoir pris connaissance, par un moyen écrit permettant d'en attester la réception.

La notification comporte les éléments prévus à l'article 33.3 du RGPD (nature de la violation, catégories et nombre approximatif de personnes et d'enregistrements concernés, conséquences probables, mesures prises ou proposées). MediWay apporte au Transporteur son assistance pour la notification éventuelle à la CNIL et aux personnes concernées.

ARTICLE 7 – TRANSFERTS HORS UNION EUROPÉENNE :

Les données sont hébergées et traitées exclusivement au sein de l'Union européenne. MediWay s'interdit tout transfert de données hors de l'Union européenne sans l'autorisation écrite préalable du Transporteur et sans les garanties prévues au chapitre V du RGPD.

ARTICLE 8 – INFORMATION ET AUDIT :

MediWay met à la disposition du Transporteur la documentation nécessaire pour démontrer le respect de ses obligations. Le Transporteur peut réaliser, à ses frais et au maximum une fois par an (sauf incident de sécurité), un audit — y compris par un tiers indépendant tenu au secret — sur pièces, moyennant un préavis de dix (10) jours ouvrés et dans le respect de la confidentialité et de la continuité de service de MediWay. En cas de sollicitation du DPO de plus d'une journée de travail, sa prestation sera facturée au Transporteur, au temps réel passé.

ARTICLE 9 – OBLIGATIONS DU TRANSPORTEUR (RESPONSABLE DE TRAITEMENT) :

Le Transporteur s'engage à :

- veiller au respect des obligations prévues par le RGPD s'agissant des traitements dont il est responsable, notamment la licéité du traitement, l'information des patients et, le cas échéant, le recueil de leur consentement ;
- s'assurer, préalablement et pendant toute la durée du traitement, du respect par MediWay des obligations prévues par le RGPD ; et
- superviser le traitement et exercer les contrôles utiles.

ARTICLE 10 – PERSONNES AGISSANT SOUS L'AUTORITÉ DU TRANSPORTEUR :

Les personnes que le Transporteur autorise à accéder à la Plateforme, notamment son Gestionnaire de flotte, ses Conducteurs et ses salariés, agissent sous son autorité et sur ses instructions au sens de l'article 29 du RGPD. Elles ne constituent pas un responsable de traitement distinct.



Le Transporteur demeure seul responsable de traitement. Il s'assure que ces personnes sont soumises à une obligation de confidentialité et de secret professionnel, encadre et révisé leurs accès à la Plateforme, et répond de leurs opérations de traitement.

Lorsque le Transporteur recourt à un prestataire externe, personne morale ou physique tierce, ce prestataire agit en qualité de sous-traitant du Transporteur ; il appartient au Transporteur de conclure avec lui un accord conforme à l'article 28 du RGPD.

ARTICLE 11 – RESPONSABILITÉ :

Chaque Partie répond des dommages causés par le traitement dans les conditions de l'article 82 du RGPD. MediWay n'est responsable que si elle n'a pas respecté les obligations du RGPD spécifiquement destinées aux sous-traitants ou si elle a agi en dehors des instructions licites du Transporteur ou contrairement à celles-ci. Les stipulations de l'article 16 des CGV s'appliquent, sous réserve des règles impératives du RGPD.

ANNEXE 1 – DESCRIPTION DES TRAITEMENTS

Responsable de traitement	Le Transporteur (identité et coordonnées figurant au Bulletin de Souscription)
Sous-traitant	MediWay, SAS — 32, avenue Paul Doumer, 75016 Paris — dpo@mediway.fr
Finalités	Gestion et optimisation du planning des Véhicules Engagés ; réception, affectation et suivi des Missions, y compris du Transport Partagé ; dématérialisation du dossier de transport (PMT, avis de passage), y compris la lecture automatisée des PMT ; prise en compte des Transports Externes renseignés par le Transporteur ; gestion des accès des Conducteurs.
Nature des opérations	Collecte, enregistrement, structuration, conservation, consultation, transmission aux Conducteurs et aux Utilisateurs concernés, mise à disposition du patient et de l'aidant, effacement.
Catégories de personnes concernées	Patients transportés ; le cas échéant, aidants ; Gestionnaire de flotte, Conducteurs et personnel du Transporteur.
Catégories de données	Données d'identification des patients (nom, prénom, date de naissance, coordonnées) ; données relatives au transport (adresses de prise en charge et de destination, dates et horaires, type de transport prescrit, horodatage de la prise en charge et de la dépose) ; données de santé strictement nécessaires figurant sur la PMT (conditions médicales du transport : position allongée, assise, etc.) ; données relatives aux Conducteurs (identité, qualifications, identifiants d'accès).
Catégories particulières (art. 9)	Données de santé (PMT) — traitement fondé sur l'article 9.2 h) du RGPD (gestion des services de soins).
Durée de conservation	Base active : les données restent accessibles dans l'application pendant trois (3) mois à compter de la réalisation du transport. Archivage intermédiaire : elles sont ensuite conservées en accès restreint (base séparée, consultation limitée et justifiée) pendant trois (3) ans, à des fins de preuve et de respect des obligations légales. Suppression définitive : à l'issue de cette période, les données sont supprimées ou anonymisées, sauf obligation légale contraire.

ANNEXE 2 – MESURES TECHNIQUES ET ORGANISATIONNELLES DE SÉCURITÉ

MediWay met en œuvre, a minima, les mesures suivantes, régulièrement réévaluées :

Mesures techniques

- chiffrement des données en transit (TLS) et au repos ;
- authentification des utilisateurs (dont mécanisme par code à usage unique / OTP) et gestion des habilitations selon le principe du moindre privilège ;



- journalisation des accès et des opérations, avec conservation et revue régulière des journaux ;
- cloisonnement des environnements, sauvegardes régulières et chiffrées, plan de reprise d'activité ;
- hébergement des données de santé auprès d'un hébergeur certifié HDS ;
- tests de sécurité et gestion des correctifs et vulnérabilités.

Mesures organisationnelles

- engagement de confidentialité du personnel et sensibilisation à la protection des données ;
- gestion documentée des accès (entrées / sorties, revue périodique) ;
- procédure de gestion des violations de données ;
- encadrement contractuel des sous-traitants ultérieurs ;
- désignation d'un point de contact « protection des données » : Maxime DELORME — dpo@mediway.fr.

ANNEXE 3 – LISTE DES SOUS-TRAITANTS ULTÉRIEURS

Sous-traitant	Prestation	Localisation des données
Hébergeur HDS : SCALINGO	Hébergement des données de santé (hébergeur certifié HDS)	Union européenne (France)
Prestataire SMS : SMSMode	Envoi des notifications aux utilisateurs par SMS	Union européenne (France)
Prestataire e-mail : Brevo	Envoi des notifications aux utilisateurs par EMAIL	Union européenne (France)
Prestataire stockage : OVHcloud	Stockage des fichiers, dont les PMT (hébergeur certifié HDS)	Union européenne (France)
Lecture des PMT : Mistral AI	Reconnaissance de caractères sur les PMT déposées	Union européenne

Cette liste est mise à jour par MediWay et communiquée au Transporteur conformément à l'article 5 du présent DPA.



Signatures

Le présent DPA est conclu en annexe des CGV et signé ou accepté dans les mêmes conditions que le Bulletin de Souscription, y compris par voie électronique conformément au Règlement (UE) n° 910/2014 (eIDAS) et aux articles 1366 et 1367 du Code civil.

Fait à {{ville}}, le {{date}},

Pour MediWay
Rebecca COHEN
Fondatrice

A handwritten signature in black ink, consisting of a stylized 'R' and 'C'.

Pour le TRANSPORTEUR
{{Dénomination}}, représenté(e) par {{Nom
Prénom}}, {{Qualité}}

Signature précédée de la mention
« Lu et approuvé, bon pour accord »

{{SIGNATURE}}



ACCORD DE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL (DPA)

Article 28 du Règlement (UE) 2016/679 (RGPD) — Annexe aux conditions générales d'utilisation MediWay — Professionnels de santé

Le présent Accord de traitement des données (ci-après le « DPA ») est annexé aux conditions générales d'utilisation de la Plateforme (les « CGU ») et en fait partie intégrante. Il est accepté en ligne par le Professionnel de santé lors de la création de son Compte. Il a pour objet d'encadrer les traitements de données à caractère personnel, en particulier de données de santé, que MediWay réalise pour le compte du Professionnel de santé au moyen de la Plateforme. Le « Professionnel de santé » désigne le médecin prescripteur ou tout autre professionnel de santé disposant d'un accès à la Plateforme ; les autres termes commençant par une majuscule ont le sens qui leur est donné dans les CGU. En cas de contradiction entre le présent DPA et les CGU s'agissant de la protection des données, le présent DPA prévaut.

ARTICLE 1 – QUALITÉ DES PARTIES :

Aux fins des traitements de données à caractère personnel relatifs aux patients et réalisés au moyen de la Plateforme pour la gestion des prescriptions médicales de transport (PMT) et l'organisation des transports sanitaires :

- le Professionnel de santé agit en qualité de responsable de traitement ; il détermine les finalités et les moyens des traitements portant sur les données de ses patients ;
- MediWay agit en qualité de sous-traitant ; elle traite ces données pour le compte et sur instructions documentées du Professionnel de santé, dans les conditions du présent DPA.

Par exception, MediWay agit en qualité de responsable de traitement autonome pour ses traitements propres qui ne sont pas réalisés pour le compte du Professionnel de santé, notamment la gestion des comptes utilisateurs et des habilitations, la sécurité et la traçabilité de la Plateforme, l'établissement de statistiques agrégées, l'amélioration de la Plateforme et la consultation, avec le consentement du Patient, de la situation de ses droits auprès de l'assurance maladie (article 12.8 des CGU). Ces traitements sont régis par la politique de confidentialité de MediWay et non par le présent DPA.

ARTICLE 2 – OBJET, DURÉE ET DESCRIPTION DES TRAITEMENTS :

Le présent DPA a pour objet de définir les conditions dans lesquelles MediWay s'engage à effectuer, pour le compte du Professionnel de santé, les opérations de traitement de données à caractère personnel décrites ci-après. La nature, la finalité, les catégories de données et de personnes concernées ainsi que la durée des traitements sont précisées en Annexe 1.

Le présent DPA prend effet à la date de son acceptation et demeure applicable pendant toute la durée des traitements réalisés pour le compte du Professionnel de santé au moyen de la Plateforme.



ARTICLE 3 – INSTRUCTIONS DOCUMENTÉES :

MediWay traite les données à caractère personnel uniquement sur instructions documentées du Professionnel de santé.

Les CGU, le paramétrage de la Plateforme et l'utilisation qui en est faite par le Professionnel de santé et les personnes agissant sous son autorité constituent les instructions initiales. MediWay informe immédiatement le Professionnel de santé si, selon elle, une instruction constitue une violation du RGPD ou d'une autre disposition applicable en matière de protection des données.

ARTICLE 4 – OBLIGATIONS DE MEDIWAY (SOUS-TRAITANT) :

MediWay s'engage à :

- ne traiter les données que pour les seules finalités faisant l'objet de la sous-traitance et conformément aux instructions documentées du Professionnel de santé ;
- garantir la confidentialité des données traitées, et veiller à ce que les personnes autorisées à les traiter s'engagent à en respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
- 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 (article 25 du RGPD) ;
- mettre en œuvre les mesures techniques et organisationnelles appropriées pour assurer la sécurité des données (article 32 du RGPD), telles que décrites en Annexe 2 ;
- héberger les données de santé auprès d'un hébergeur de données de santé (HDS) certifié conformément à l'article L.1111-8 du Code de la santé publique ;
- assister le Professionnel de santé, compte tenu de la nature du traitement, dans l'exercice par les patients de leurs droits (accès, rectification, effacement, opposition, limitation, portabilité) ;
- aider le Professionnel de santé à garantir le respect de ses obligations en matière de sécurité, de notification des violations, d'analyse d'impact (AIPD) et de consultation préalable de la CNIL ;
- mettre à la disposition du Professionnel de santé toutes les informations nécessaires pour démontrer le respect des obligations de l'article 28 du RGPD et permettre la réalisation d'audits, dans les conditions de l'article 8 ;
- tenir un registre de toutes les catégories d'activités de traitement effectuées pour le compte du Professionnel de santé, conformément à l'article 30.2 du RGPD ;
- au terme des traitements, et au choix du Professionnel de santé, supprimer les données ou les lui restituer, puis détruire les copies existantes, sauf obligation légale de conservation, dans les conditions de durée prévues en Annexe 1.

ARTICLE 5 – SOUS-TRAITANCE ULTÉRIEURE :

Le Professionnel de santé autorise de manière générale MediWay à recourir à des sous-traitants ultérieurs pour l'exécution des services, notamment pour l'hébergement des données de santé, le stockage des fichiers, la lecture automatisée des PMT et l'envoi de notifications. La liste des sous-traitants ultérieurs en vigueur figure en Annexe 3.

MediWay informe le Professionnel de santé de tout ajout ou remplacement d'un sous-traitant ultérieur, par écrit et au moins trente (30) jours à l'avance ; le Professionnel de santé peut formuler des objections pendant ce délai. MediWay impose à chaque sous-traitant ultérieur, par contrat, les mêmes obligations de protection des données que celles prévues au présent DPA, et demeure pleinement responsable envers le Professionnel de santé de leur exécution.



ARTICLE 6 – SÉCURITÉ ET VIOLATION DE DONNÉES :

MediWay met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, en tenant compte notamment du caractère des données de santé (chiffrement, contrôle des accès, journalisation, sauvegardes, cloisonnement — voir Annexe 2).

En cas de violation avérée de données à caractère personnel, MediWay notifie le Professionnel de santé dans les meilleurs délais et au plus tard quarante-huit (48) heures après en avoir pris connaissance, par un moyen écrit permettant d'en attester la réception.

La notification comporte les éléments prévus à l'article 33.3 du RGPD (nature de la violation, catégories et nombre approximatif de personnes et d'enregistrements concernés, conséquences probables, mesures prises ou proposées). MediWay apporte au Professionnel de santé son assistance pour la notification éventuelle à la CNIL et aux personnes concernées.

ARTICLE 7 – TRANSFERTS HORS UNION EUROPÉENNE :

Les données sont hébergées et traitées exclusivement au sein de l'Union européenne. MediWay s'interdit tout transfert de données hors de l'Union européenne sans l'autorisation écrite préalable du Professionnel de santé et sans les garanties prévues au chapitre V du RGPD.

ARTICLE 8 – INFORMATION ET AUDIT :

MediWay met à la disposition du Professionnel de santé la documentation nécessaire pour démontrer le respect de ses obligations. Le Professionnel de santé peut réaliser, à ses frais et au maximum une fois par an (sauf incident de sécurité), un audit — y compris par un tiers indépendant tenu au secret — sur pièces, moyennant un préavis de dix (10) jours ouvrés et dans le respect de la confidentialité et de la continuité de service de MediWay. En cas de sollicitation du DPO de plus d'une journée de travail, sa prestation sera facturée au Professionnel de santé, au temps réel passé.

ARTICLE 9 – OBLIGATIONS DU PROFESSIONNEL DE SANTÉ (RESPONSABLE DE TRAITEMENT) :

Le Professionnel de santé s'engage à :

- veiller au respect des obligations prévues par le RGPD s'agissant des traitements dont il est responsable, notamment la licéité du traitement, l'information des patients et, le cas échéant, le recueil de leur consentement ;
- s'assurer, préalablement et pendant toute la durée du traitement, du respect par MediWay des obligations prévues par le RGPD ; et
- superviser le traitement et exercer les contrôles utiles.

ARTICLE 10 – PERSONNES AGISSANT SOUS L'AUTORITÉ DU PROFESSIONNEL DE SANTÉ :

Lorsque le Professionnel de santé autorise son secrétariat médical, ou tout membre de son personnel (infirmier, remplaçant), à accéder à la Plateforme pour déposer les PMT et réserver les transports, ces personnes agissent sous son autorité et sur ses instructions au sens de l'article 29 du RGPD. Elles ne constituent pas un responsable de traitement distinct.



Le Professionnel de santé demeure seul responsable de traitement. Il s'assure que ces personnes sont soumises à une obligation de confidentialité et de secret professionnel, encadre et révisé leurs accès à la Plateforme, et répond de leurs opérations de traitement.

Lorsque le Professionnel de santé recourt à un secrétariat externalisé constituant une personne morale ou physique tierce, ce prestataire agit en qualité de sous-traitant du Professionnel de santé ; il appartient au Professionnel de santé de conclure avec lui un accord conforme à l'article 28 du RGPD.

ARTICLE 11 – RESPONSABILITÉ :

Chaque Partie répond des dommages causés par le traitement dans les conditions de l'article 82 du RGPD. MediWay n'est responsable que si elle n'a pas respecté les obligations du RGPD spécifiquement destinées aux sous-traitants ou si elle a agi en dehors des instructions licites du Professionnel de santé ou contrairement à celles-ci. Les stipulations de l'article 9 des CGU s'appliquent, sous réserve des règles impératives du RGPD.

ANNEXE 1 – DESCRIPTION DES TRAITEMENTS

Responsable de traitement	Le Professionnel de santé (identité et coordonnées renseignées lors de la création du Compte)
Sous-traitant	MediWay, SAS — 32, avenue Paul Doumer, 75016 Paris — dpo@mediway.fr
Finalités	Gestion et dépôt des prescriptions médicales de transport (PMT), y compris leur lecture automatisée ; recherche et mise en relation avec les transporteurs disponibles ; réservation et suivi des transports sanitaires ; génération des avis de passage et documents associés.
Nature des opérations	Collecte, enregistrement, structuration, conservation, consultation, transmission aux transporteurs concernés, mise à disposition du patient et de l'aidant, effacement.
Catégories de personnes concernées	Patients du Professionnel de santé ; le cas échéant, aidants désignés.
Catégories de données	Données d'identification (nom, prénom, date de naissance, coordonnées) ; données relatives au transport (adresses de prise en charge et de destination, dates/horaires, type de transport prescrit) ; données de santé strictement nécessaires figurant sur la PMT (conditions médicales du transport : position allongée, assise, etc.).
Catégories particulières (art. 9)	Données de santé (PMT) — traitement fondé sur l'article 9.2 h) du RGPD (gestion des services de soins).
Durée de conservation	Base active : les données restent accessibles dans l'application pendant trois (3) mois à compter de la réalisation du transport. Archivage intermédiaire : elles sont ensuite conservées en accès restreint (base séparée, consultation limitée et justifiée) pendant trois (3) ans, à des fins de preuve et de respect des obligations légales. Suppression définitive : à l'issue de cette période, les données sont supprimées ou anonymisées, sauf obligation légale contraire.

ANNEXE 2 – MESURES TECHNIQUES ET ORGANISATIONNELLES DE SÉCURITÉ

MediWay met en œuvre, a minima, les mesures suivantes, régulièrement réévaluées :

Mesures techniques

- chiffrement des données en transit (TLS) et au repos ;
- authentification des utilisateurs (dont mécanisme par code à usage unique / OTP) et gestion des habilitations selon le principe du moindre privilège ;
- journalisation des accès et des opérations, avec conservation et revue régulière des journaux ;
- cloisonnement des environnements, sauvegardes régulières et chiffrées, plan de reprise d'activité ;
- hébergement des données de santé auprès d'un hébergeur certifié HDS ;



- tests de sécurité et gestion des correctifs et vulnérabilités.

Mesures organisationnelles

- engagement de confidentialité du personnel et sensibilisation à la protection des données ;
- gestion documentée des accès (entrées / sorties, revue périodique) ;
- procédure de gestion des violations de données ;
- encadrement contractuel des sous-traitants ultérieurs ;
- désignation d'un point de contact « protection des données » : Maxime DELORME — dpo@mediway.fr.

ANNEXE 3 – LISTE DES SOUS-TRAITANTS ULTÉRIEURS

Sous-traitant	Prestation	Localisation des données
Hébergeur HDS : SCALINGO	Hébergement des données de santé (hébergeur certifié HDS)	Union européenne (France)
Prestataire SMS : SMSMode	Envoi des notifications aux utilisateurs par SMS	Union européenne (France)
Prestataire e-mail : Brevo	Envoi des notifications aux utilisateurs par EMAIL	Union européenne (France)
Prestataire stockage : OVHcloud	Stockage des fichiers, dont les PMT (hébergeur certifié HDS)	Union européenne (France)
Lecture des PMT : Mistral AI	Reconnaissance de caractères sur les PMT déposées	Union européenne

Cette liste est mise à jour par MediWay et communiquée au Professionnel de santé conformément à l'article 5 du présent DPA.



Acceptation

Le présent DPA est accepté en ligne par le Professionnel de santé, par une case à cocher distincte, lors de la création de son Compte. Cette acceptation est enregistrée et horodatée par la Plateforme ; elle vaut consentement au présent DPA, conformément aux articles 1366 et 1367 du Code civil et au Règlement (UE) n° 910/2014 (eIDAS).



ACCORD DE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL (DPA)

Article 28 du Règlement (UE) 2016/679 (RGPD) — Annexe aux conditions générales d'utilisation MediWay —
Établissements de santé

Le présent Accord de traitement des données (ci-après le « DPA ») est annexé aux conditions générales d'utilisation de la Plateforme (les « CGU ») et en fait partie intégrante. Il est accepté en ligne, lors de la création de l'environnement de l'Établissement de santé sur la Plateforme, par son représentant habilité dans les conditions de l'article 4.3 des CGU. Il s'applique également à toute licence ou convention conclue ultérieurement entre MediWay et l'Établissement de santé, sauf stipulation contraire. Il a pour objet d'encadrer les traitements de données à caractère personnel, en particulier de données de santé, que MediWay réalise pour le compte de l'Établissement de santé au moyen de la Plateforme. Les termes commençant par une majuscule ont le sens qui leur est donné dans les CGU. En cas de contradiction entre le présent DPA et les CGU s'agissant de la protection des données, le présent DPA prévaut.

ARTICLE 1 – QUALITÉ DES PARTIES :

Aux fins des traitements de données à caractère personnel relatifs aux patients et réalisés au moyen de la Plateforme pour la gestion des prescriptions médicales de transport (PMT) et l'organisation des transports sanitaires :

- l'Établissement de santé agit en qualité de responsable de traitement ; il détermine les finalités et les moyens des traitements portant sur les données de ses patients ;
- MediWay agit en qualité de sous-traitant ; elle traite ces données pour le compte et sur instructions documentées de l'Établissement de santé, dans les conditions du présent DPA.

Par exception, MediWay agit en qualité de responsable de traitement autonome pour ses traitements propres qui ne sont pas réalisés pour le compte de l'Établissement de santé, notamment la gestion des comptes utilisateurs et des habilitations, la sécurité et la traçabilité de la Plateforme, l'établissement de statistiques agrégées, l'amélioration de la Plateforme et la consultation, avec le consentement du Patient, de la situation de ses droits auprès de l'assurance maladie (article 12.8 des CGU). Ces traitements sont régis par la politique de confidentialité de MediWay et non par le présent DPA.

ARTICLE 2 – OBJET, DURÉE ET DESCRIPTION DES TRAITEMENTS :

Le présent DPA a pour objet de définir les conditions dans lesquelles MediWay s'engage à effectuer, pour le compte de l'Établissement de santé, les opérations de traitement de données à caractère personnel décrites ci-après. La nature, la finalité, les catégories de données et de personnes concernées ainsi que la durée des traitements sont précisées en Annexe 1.



Le présent DPA prend effet à la date de son acceptation et demeure applicable pendant toute la durée des traitements réalisés pour le compte de l'Établissement de santé au moyen de la Plateforme.

ARTICLE 3 – INSTRUCTIONS DOCUMENTÉES :

MediWay traite les données à caractère personnel uniquement sur instructions documentées de l'Établissement de santé.

Les CGU, le paramétrage de la Plateforme et l'utilisation qui en est faite par l'Établissement de santé et les personnes agissant sous son autorité constituent les instructions initiales. MediWay informe immédiatement l'Établissement de santé si, selon elle, une instruction constitue une violation du RGPD ou d'une autre disposition applicable en matière de protection des données.

ARTICLE 4 – OBLIGATIONS DE MEDIWAY (SOUS-TRAITANT) :

MediWay s'engage à :

- ne traiter les données que pour les seules finalités faisant l'objet de la sous-traitance et conformément aux instructions documentées de l'Établissement de santé ;
- garantir la confidentialité des données traitées, et veiller à ce que les personnes autorisées à les traiter s'engagent à en respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
- 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 (article 25 du RGPD) ;
- mettre en œuvre les mesures techniques et organisationnelles appropriées pour assurer la sécurité des données (article 32 du RGPD), telles que décrites en Annexe 2 ;
- héberger les données de santé auprès d'un hébergeur de données de santé (HDS) certifié conformément à l'article L.1111-8 du Code de la santé publique ;
- assister l'Établissement de santé, compte tenu de la nature du traitement, dans l'exercice par les patients de leurs droits (accès, rectification, effacement, opposition, limitation, portabilité) ;
- aider l'Établissement de santé à garantir le respect de ses obligations en matière de sécurité, de notification des violations, d'analyse d'impact (AIPD) et de consultation préalable de la CNIL ;
- mettre à la disposition de l'Établissement de santé toutes les informations nécessaires pour démontrer le respect des obligations de l'article 28 du RGPD et permettre la réalisation d'audits, dans les conditions de l'article 8 ;
- tenir un registre de toutes les catégories d'activités de traitement effectuées pour le compte de l'Établissement de santé, conformément à l'article 30.2 du RGPD ;
- au terme des traitements, et au choix de l'Établissement de santé, supprimer les données ou les lui restituer, puis détruire les copies existantes, sauf obligation légale de conservation, dans les conditions de durée prévues en Annexe 1.

ARTICLE 5 – SOUS-TRAITANCE ULTÉRIEURE :

L'Établissement de santé autorise de manière générale MediWay à recourir à des sous-traitants ultérieurs pour l'exécution des services, notamment pour l'hébergement des données de santé, le stockage des fichiers,



la lecture automatisée des PMT et l'envoi de notifications. La liste des sous-traitants ultérieurs en vigueur figure en Annexe 3.

MediWay informe l'Établissement de santé de tout ajout ou remplacement d'un sous-traitant ultérieur, par écrit et au moins trente (30) jours à l'avance ; l'Établissement de santé peut formuler des objections pendant ce délai. MediWay impose à chaque sous-traitant ultérieur, par contrat, les mêmes obligations de protection des données que celles prévues au présent DPA, et demeure pleinement responsable envers l'Établissement de santé de leur exécution.

ARTICLE 6 – SÉCURITÉ ET VIOLATION DE DONNÉES :

MediWay met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, en tenant compte notamment du caractère des données de santé (chiffrement, contrôle des accès, journalisation, sauvegardes, cloisonnement — voir Annexe 2).

En cas de violation avérée de données à caractère personnel, MediWay notifie l'Établissement de santé dans les meilleurs délais et au plus tard quarante-huit (48) heures après en avoir pris connaissance, par un moyen écrit permettant d'en attester la réception.

La notification comporte les éléments prévus à l'article 33.3 du RGPD (nature de la violation, catégories et nombre approximatif de personnes et d'enregistrements concernés, conséquences probables, mesures prises ou proposées). MediWay apporte à l'Établissement de santé son assistance pour la notification éventuelle à la CNIL et aux personnes concernées.

ARTICLE 7 – TRANSFERTS HORS UNION EUROPÉENNE :

Les données sont hébergées et traitées exclusivement au sein de l'Union européenne. MediWay s'interdit tout transfert de données hors de l'Union européenne sans l'autorisation écrite préalable de l'Établissement de santé et sans les garanties prévues au chapitre V du RGPD.

ARTICLE 8 – INFORMATION ET AUDIT :

MediWay met à la disposition de l'Établissement de santé la documentation nécessaire pour démontrer le respect de ses obligations. L'Établissement de santé peut réaliser, à ses frais et au maximum une fois par an (sauf incident de sécurité), un audit — y compris par un tiers indépendant tenu au secret — sur pièces, moyennant un préavis de dix (10) jours ouvrés et dans le respect de la confidentialité et de la continuité de service de MediWay. En cas de sollicitation du DPO de plus d'une journée de travail, sa prestation sera facturée à l'Établissement de santé, au temps réel passé.



ARTICLE 9 – OBLIGATIONS DE L'ÉTABLISSEMENT DE SANTÉ (RESPONSABLE DE TRAITEMENT) :

L'Établissement de santé s'engage à :

- veiller au respect des obligations prévues par le RGPD s'agissant des traitements dont il est responsable, notamment la licéité du traitement, l'information des patients et, le cas échéant, le recueil de leur consentement ;
- s'assurer, préalablement et pendant toute la durée du traitement, du respect par MediWay des obligations prévues par le RGPD ; et
- superviser le traitement et exercer les contrôles utiles.

ARTICLE 10 – PERSONNES AGISSANT SOUS L'AUTORITÉ DE L'ÉTABLISSEMENT DE SANTÉ :

Les personnes que l'Établissement de santé autorise à accéder à la Plateforme, notamment ses médecins, personnels soignants, secrétariats et services chargés de l'organisation des transports, agissent sous son autorité et sur ses instructions au sens de l'article 29 du RGPD. Elles ne constituent pas un responsable de traitement distinct.

L'Établissement de santé demeure seul responsable de traitement. Il s'assure que ces personnes sont soumises à une obligation de confidentialité et de secret professionnel, encadre et révisé leurs accès à la Plateforme, et répond de leurs opérations de traitement.

Lorsque l'Établissement de santé recourt à un prestataire externe, personne morale ou physique tierce, ce prestataire agit en qualité de sous-traitant de l'Établissement de santé ; il appartient à l'Établissement de santé de conclure avec lui un accord conforme à l'article 28 du RGPD.

ARTICLE 11 – RESPONSABILITÉ :

Chaque Partie répond des dommages causés par le traitement dans les conditions de l'article 82 du RGPD. MediWay n'est responsable que si elle n'a pas respecté les obligations du RGPD spécifiquement destinées aux sous-traitants ou si elle a agi en dehors des instructions licites de l'Établissement de santé ou contrairement à celles-ci. Les stipulations de l'article 9 des CGU s'appliquent, sous réserve des règles impératives du RGPD.



ANNEXE 1 – DESCRIPTION DES TRAITEMENTS

Responsable de traitement	L'Établissement de santé (identité et coordonnées renseignées lors de la création de son environnement sur la Plateforme)
Sous-traitant	MediWay, SAS — 32, avenue Paul Doumer, 75016 Paris — dpo@mediway.fr
Finalités	Gestion et dépôt des prescriptions médicales de transport (PMT), y compris leur lecture automatisée ; recherche et mise en relation avec les transporteurs disponibles ; réservation et suivi des transports sanitaires ; génération des avis de passage et documents associés.
Nature des opérations	Collecte, enregistrement, structuration, conservation, consultation, transmission aux transporteurs concernés, mise à disposition du patient et de l'aidant, effacement.
Catégories de personnes concernées	Patients de l'Établissement de santé ; le cas échéant, aidants désignés.
Catégories de données	Données d'identification (nom, prénom, date de naissance, coordonnées) ; données relatives au transport (adresses de prise en charge et de destination, dates/horaires, type de transport prescrit) ; données de santé strictement nécessaires figurant sur la PMT (conditions médicales du transport : position allongée, assise, etc.).
Catégories particulières (art. 9)	Données de santé (PMT) — traitement fondé sur l'article 9.2 h) du RGPD (gestion des services de soins).
Durée de conservation	Base active : les données restent accessibles dans l'application pendant trois (3) mois à compter de la réalisation du transport. Archivage intermédiaire : elles sont ensuite conservées en accès restreint (base séparée, consultation limitée et justifiée) pendant trois (3) ans, à des fins de preuve et de respect des obligations légales. Suppression définitive : à l'issue de cette période, les données sont supprimées ou anonymisées, sauf obligation légale contraire.

ANNEXE 2 – MESURES TECHNIQUES ET ORGANISATIONNELLES DE SÉCURITÉ

MediWay met en œuvre, a minima, les mesures suivantes, régulièrement réévaluées :

Mesures techniques

- chiffrement des données en transit (TLS) et au repos ;
- authentification des utilisateurs (dont mécanisme par code à usage unique / OTP) et gestion des habilitations selon le principe du moindre privilège ;
- journalisation des accès et des opérations, avec conservation et revue régulière des journaux ;
- cloisonnement des environnements, sauvegardes régulières et chiffrées, plan de reprise d'activité ;
- hébergement des données de santé auprès d'un hébergeur certifié HDS ;
- tests de sécurité et gestion des correctifs et vulnérabilités.

Mesures organisationnelles

- engagement de confidentialité du personnel et sensibilisation à la protection des données ;
- gestion documentée des accès (entrées / sorties, revue périodique) ;
- procédure de gestion des violations de données ;



- encadrement contractuel des sous-traitants ultérieurs ;
- désignation d'un point de contact « protection des données » : Maxime DELORME — dpo@mediway.fr.

ANNEXE 3 – LISTE DES SOUS-TRAITANTS ULTÉRIEURS

Sous-traitant	Prestation	Localisation des données
Hébergeur HDS : SCALINGO	Hébergement des données de santé (hébergeur certifié HDS)	Union européenne (France)
Prestataire SMS : SMSMode	Envoi des notifications aux utilisateurs par SMS	Union européenne (France)
Prestataire e-mail : Brevo	Envoi des notifications aux utilisateurs par EMAIL	Union européenne (France)
Prestataire stockage : OVHcloud	Stockage des fichiers, dont les PMT (hébergeur certifié HDS)	Union européenne (France)
Lecture des PMT : Mistral AI	Reconnaissance de caractères sur les PMT déposées	Union européenne

Cette liste est mise à jour par MediWay et communiquée à l'Établissement de santé conformément à l'article 5 du présent DPA.



Acceptation

Le présent DPA est accepté en ligne par le représentant habilité de l'Établissement de santé, par une case à cocher distincte, lors de la création de l'environnement de l'Établissement de santé sur la Plateforme. Cette acceptation est enregistrée et horodatée par la Plateforme ; elle vaut consentement au présent DPA, conformément aux articles 1366 et 1367 du Code civil et au Règlement (UE) n° 910/2014 (eIDAS).