Politique sur les données de Renault Group

1. Le Règlement européen sur les données et la présente Politique.

L'objectif du Règlement (EU) 2023/2854 sur les données (ci-après, le « Règlement »), qui entre en application le 12 septembre 2025, est de faciliter la circulation des données générées par les produits connectés et les services connexes afin d'accroître l'innovation et la croissance économique au sein de l'Union européenne.

Ce Règlement donne aux utilisateurs de produits connectés et de services connexes un **droit d'accès** à certaines données générées par ces produits et services ainsi qu'un **droit de partage** de ces données à des tiers.

À titre d'exemple, le Règlement pourrait permettre à l'utilisateur d'un véhicule connecté fabriqué par Renault d'accéder aux données relatives au kilométrage de son véhicule qui ont été extraites de celui-ci et qui sont disponibles sur le serveur de Renault, afin de les partager avec son garagiste ou sa compagnie d'assurance, sous certaines conditions.

La présente Politique reflète l'application des règles édictées par le Règlement aux activités concernées au sein de Renault Group.

2. Qu'est-ce qu'un produit connecté et un service connexe ?

Un **produit connecté** est un produit (tel qu'un véhicule) qui obtient, génère ou recueille des données sur son utilisation ou son environnement et peut communiquer ces données par l'intermédiaire d'un service de communications électroniques, d'une connexion physique ou d'un dispositif d'accès intégré (tels que le Wifi ou le Bluetooth ou encore un réseau internet mobile). Sont exclus de cette définition les produits dont la fonction principale est de stocker, de traiter ou de transmettre ces données pour le compte d'autres parties que l'utilisateur (tels que les serveurs exploités entièrement pour le compte de tiers).

Par exemple, un véhicule fabriqué par Renault dont certaines données peuvent être consultées sur l'application my Renault ou tout autre moyen informatique est un produit connecté.

Un **service connexe** est :

- un service numérique, à l'exclusion des services de communications électroniques (tels qu'un service d'accès à l'internet),
- connecté au produit au moment de l'achat ou de la mise en location ou en crédit-bail, et
- indispensable à l'exécution d'une ou plusieurs de ses fonctions.

Il peut également s'agir d'un service qui est ensuite connecté au produit par le fabricant ou par un tiers pour ajouter, mettre à jour ou adapter les fonctions du produit connecté.

Par exemple, les services de programmation de charge à distance et de chauffage à distance disponibles sur l'application my Renault sont des services connexes.

3. À qui s'applique la présente Politique ?

Cette Politique s'applique :

- à Renault ou, potentiellement, l'une de ses filiales, lorsque Renault et/ou l'une de ses filiales est **détenteur de données** au sens du Règlement (ci-après, « Renault » ou « nous »),

- à tout **utilisateur** de produits connectés ou de services connexes dont Renault détient les données au sens du Règlement, et

- à tout **tiers** désigné par un utilisateur pour recevoir de la part de Renault les données facilement accessibles (ci-après, le « tiers » ou, lorsque ce tiers agit à des fins professionnelles, le « destinataire de données », étant précisé que le destinataire de données peut également recevoir des données de la part de Renault conformément à une autre obligation légale).

Renault est détenteur de données lorsqu'elle a le droit ou l'obligation d'utiliser et de mettre à disposition des données en vertu d'une obligation légale ou contractuelle.

L'utilisateur est toute personne physique ou morale :

- qui est propriétaire d'un produit connecté, tel qu'un véhicule ou une borne de recharge connectés fabriqués par Renault, ou

- à laquelle des droits temporaires d'utilisation d'un produit connecté ont été cédés contractuellement (par exemple, dans le cadre d'une location ou d'un crédit-bail), ou

- qui reçoit un service connexe.

4. Quel est l'objectif de la Politique sur les données ?

La Politique sur les données définit les droits et obligations des détenteurs, utilisateurs et des tiers (y compris les destinataires de données) en application du Règlement.

Cette Politique est complétée le cas échéant par les dispositions particulières contenues dans les contrats conclus entre Renault et les utilisateurs et les tiers. En cas de conflit entre l'une de ces dispositions et la présente Politique, la disposition contractuelle prévaut.

Cette Politique s'ajoute à nos politiques en matière de protection de vos données personnelles. En cas de conflit entre la présente Politique et nos politiques en matière de protection de vos données personnelles, ces dernières prévalent.

5. À quelles données les utilisateurs ont-ils accès ?

Les utilisateurs ont accès :

- aux données personnelles et non personnelles générées par l'utilisation d'un produit connecté, tel qu'un véhicule connecté fabriqué par Renault, dès lors qu'elles ont été conçues pour être extraites par un utilisateur, un détenteur de données ou un tiers au moyen d'un service de communications électroniques, d'une connexion physique ou d'un dispositif d'accès intégré (par exemple les données de kilométrage du véhicule connecté) ;

- aux données personnelles et non personnelles représentant les actions de l'utilisateur ou les événements liés au produit connecté, que l'utilisateur a enregistrées intentionnellement ou qui résultent indirectement de l'action de l'utilisateur lors de la fourniture d'un service connexe (par exemple, une demande de charge à distance dans l'application My Renault) ; et

- aux métadonnées pertinentes et nécessaires à l'interprétation et l'utilisation de ces données (par exemple, l'heure et la date de chaque donnée remontée).

L'utilisateur a uniquement accès à ces données dans la mesure où Renault les a obtenues ou peut les obtenir légalement à partir d'un produit connecté ou d'un service connexe, sans effort disproportionné allant au-delà d'une simple opération (ci-après, les « données facilement accessibles »).

En outre, l'utilisateur a uniquement accès aux données « brutes » ou « primaires » c'est-à-dire générées automatiquement sans autre forme de traitement que celui de les rendre compréhensibles et utilisables. À l'inverse, l'utilisateur n'a pas accès aux données dites « dérivées » qui sont le résultat d'un investissement supplémentaire de la part du détenteur de données (pour valoriser les données brutes notamment en ayant recours à des algorithmes complexes).

Enfin, il existe des règles spécifiques énumérées ci-après concernant certains types de données :

Type de données	Définition	Exemple(s)	Règles
Données relatives à la sécurité d'un produit connecté	Les données dont le traitement est susceptible de porter atteinte aux exigences de la sécurité d'un produit connecté entraînant de graves effets indésirables pour la santé, la sûreté ou la sécurité des personnes.	• Données relatives aux composantes sécuritaires du véhicule • Données utilisées pour détecter des intrusions dans le véhicule • Données pour prévenir une modification du système de contrôle des émissions	Nous pouvons contractuellement restreindre ou interdire l'accès à ces données, leur utilisation ou leur partage ultérieur.
Données protégées en tant que secrets d'affaires	Les données qui constituent des informations secrètes, ont une valeur commerciale et font l'objet de mesures pour être maintenues secrètes.	• Données révélant le fonctionnement d'une technologie secrète déployée par Renault	Les données protégées en tant que secrets d'affaires sont préservées et ne seront divulguées que lorsque Renault prendra conjointement avec l'utilisateur toutes les mesures nécessaires avant la divulgation pour préserver leur confidentialité (par exemple des mesures de cryptage, pare-feu etc.).

			Renault ou le détenteur de secrets d'affaires recense les données protégées par les secrets d'affaires et convient avec l'utilisateur de mesures techniques et organisationnelles proportionnées nécessaires afin de préserver la confidentialité des données partagées par le biais de clauses contractuelles types ou autres types d'accords. En l'absence d'accord sur les mesures nécessaires, ou si l'utilisateur ne met pas en œuvre les mesures convenues ou compromet la confidentialité des secrets d'affaires, Renault peut bloquer ou, selon le cas, suspendre le partage des données définies comme secrets d'affaires. Notre décision sera motivée et communiquée par écrit à l'utilisateur sans retard injustifié. Dans des circonstances exceptionnelles, lorsque nous pouvons démontrer qu'il est très probable que la divulgation des secrets d'affaires engendre un préjudice économique grave, malgré les mesures prises par l'utilisateur, Renault peut refuser au cas par cas une demande d'accès aux données spécifiques en question. Cette démonstration est basée sur des éléments objectifs.
Données personnelles concernant une autre personne que l'utilisateur	Les données qui se rapportent à une personne physique identifiée ou identifiable au sens du RGPD, autre que l'utilisateur, générées par l'utilisation d'un produit connecté ou	• Données issues des caméras du véhicule filmant des passants	Ces données ne sont mises à la disposition de l'utilisateur que s'il existe un fondement juridique valable en application du RGPD pour ce faire et que, le cas échéant, les conditions relatives aux données sensibles et aux traceurs et cookies sont respectées.

	d'un service connexe.		
Données protégées par des droits de propriété intellectuelle	Les données protégées par un droit d'auteur, un droit de marque, un brevet, un dessin ou un modèle, à l'exception du droit de protection des bases de données.	• Données liées au contenu affiché ou lu par l'utilisateur, tel que la musique que l'utilisateur écoute dans son véhicule	L'utilisateur n'a pas de droit d'accès ou de partage de ces données.

Pour donner une illustration des types de données susceptibles d'être générées par l'usage des véhicules connectés et services associés, vous trouverez ci-dessous une liste non exhaustive fournie à titre d'exemple.

Nous tenons à rappeler que seules les données déjà générées par le véhicule sont concernées, celles-ci dépendant, sans toutefois s'y limiter :

- de la version, de l'équipement, du type d'utilisation, des modifications et des réservations de services digitaux ;

- des services que l'utilisateur a activés dans son véhicule ;

- des choix que l'utilisateur a exprimés dans les paramètres de confidentialité de son véhicule.

Comme rappelé plus haut, nous tenons aussi à rappeler que parmi ces données fournies à titre d'exemple, **seules les données « brutes » ou « primaires » c'est-à-dire générées automatiquement sans autre forme de traitement que celui de les rendre compréhensibles et utilisables sont concernées**.

Catégorie	Exemples de données
Données de géolocalisation du véhicule	• Position du véhicule en début et fin de trajet • Position du véhicule durant le trajet, toutes les 3 secondes • Localisation d'événements particuliers : coups de frein brusques, coups de volants brusques, déclenchement d'ABS, du freinage d'urgence, déclenchement des airbags, etc.
Données relatives à un trajet	• Kilométrage parcouru • Durée du trajet • Date / jour / horaire du trajet • Consommation sur le trajet
Données relatives à un événement de charge du véhicule	• Quantité d'énergie chargée • Type de charge • Type de borne (AC / DC) • Puissance moyenne de charge

	• Horaire de début et de fin de charge
Données de conduite	• Vitesses, accélérations longitudinales et transversales • Appuis pédales de frein, d'accélérateur et d'embrayage • Vitesse de rotation volant • Position du levier de vitesse • Utilisation des palettes au volant
Données relatives à l'utilisation des fonctions secondaires du véhicule	• Utilisation des essuie-glaces • Utilisation des feux de route et feux de croisement • Utilisation des clignotants • Choix des modes de conduite
Données relatives à l'utilisation des ouvrants et à l'occupation du véhicule	• Ouverture des portières • Détection de la présence de conducteurs et de passagers • Détection des bouclages ceinture • Ouverture des vitres
Données relatives à l'utilisation des fonctions de confort thermique du véhicule	• Utilisation de la climatisation et du chauffage : activation, température de consigne, ventilation
Données relatives aux conditions météorologiques	• Température extérieure • Capteur de pluie • Capteur de luminosité
Données relatives à l'état du véhicule	• Kilométrage véhicule (Distance Totalizer) • Alerte vidange ou visite d'entretien • Alerte niveau de carburant • Alerte niveau d'urée • Voyant d'alerte 'MIL ON' • Failure système : ABS, AFU, ESC, Airbag • Détection de crash
Données relatives à la pression des pneus	• Mesure pression des pneus (mesure directe)
Données relatives à l'activation des systèmes	• Mesure des couples et vitesses volants • Occurrences d'activation du système de freinage • Durées d'activation du système de freinage • Pression de freinage
Données relatives au moteur et à l'état des systèmes	• Couples / régimes moteur • Température de refroidissement • Etat de charge filtre à particule • Tension des cellules batterie • Température batterie • Energie totale consommée

	• Etat de santé batterie • Température refroidissement batterie • Courant batterie • Alerte température batterie • SOC batterie 12 V

Les données générées par l'usage du produit connecté ou du service connexe sont accessibles en continu dans un format distinct en fonction de la qualité de l'Utilisateur (personne morale ou personne physique) :

- API (Application Programming Interface ou Interface de programmation d'application) qui est une interface logicielle permettant de connecter un logiciel ou un service à un autre logiciel ou service afin d'échanger des données et des fonctionnalités.

- JSON (Javascript Object Notation) qui est un format texte permettant de stocker et d'échanger des données de manière lisible par l'utilisateur et analysable par machine.

Les données générées sont conservées pendant la durée nécessaire aux finalités de l'utilisation éventuelle des données par Renault.

Le volume de données générées dépend notamment du modèle de véhicule connecté, de la configuration du véhicule connecté, des services connectés activés, de l'intensité d'usage du véhicule connecté (fréquence, durée et conditions d'utilisation, localisation du véhicule, état d'entretien du véhicule). A titre d'exemple, un véhicule de type CLIO hybride ou Renault 5 peut générer en moyenne près de 25 Mo de données par mois, pour un usage d'environ 1000 km mensuels en France (volume estimatif).

6. Comment l'utilisateur peut-il accéder à ces données ?

6.1 L'utilisateur personne physique peut accéder aux données via un fichier JSON qu'il peut télécharger au moyen d'un lien sécurisé.

L'utilisateur personne physique doit au préalable disposer d'un compte MyRenault, MyDacia, MyAlpine ou MyDuo et associer son véhicule à son compte.

L'utilisateur accède au site web de la marque de son véhicule (ex. renault.fr, dacia.it) et, dans le footer, clique sur la Section « Data Act » pour ouvrir la rubrique « Nos politiques sur les données ».

Dans la Section « Information spécifique : le règlement sur les données (Data Act) », l'utilisateur sélectionne « Gérer l'accès à vos données ».

Sur la page « Accès et partage des données véhicule », l'utilisateur clique sur « Demander mes données ».

L'utilisateur se connecte avec ses identifiants MyRenault, MyDacia, MyAlpine ou MyDuo pour demander l'accès.

Après soumission de sa demande, l'utilisateur reçoit un courriel pour la finaliser : il doit renseigner le VIN, sélectionner les catégories de données et la période concernée, certifier être le conducteur du véhicule sur la période indiquée et accepter les conditions générales d'accès ou, en cas de

partage avec un tiers, confirmer son autorisation au partage ainsi que les coordonnées du tiers autorisé.

L'utilisateur reçoit par courriel un lien sécurisé lui permettant de télécharger un fichier contenant les données sélectionnées.

6.2 L'utilisateur personne morale peut accéder aux données sous forme de fichier JSON ou d'API.

Pour ce faire, l'utilisateur personne morale pourra contacter Renault via le formulaire de demande d'information disponible dans la Section « Data Act » accessible via le footer du site web de la marque.

6.3 Si la demande de l'utilisateur remplit les conditions légales applicables, nous lui transmettrons les données facilement accessibles et les métadonnées associées :

- sans retard injustifié après que les données ont été accessibles à Renault,
- à un niveau de qualité identique à celui dont bénéficie Renault,
- de manière aisée et sécurisée,
- dans un format complet, structuré, couramment utilisé et lisible par machine (tel que API ou Streaming) et,
- si pertinent et techniquement possible, en continu et en temps réel.

Toute demande de communication de données de la part d'un utilisateur est gratuite.

7. À qui l'utilisateur peut-il communiquer ces données ?

Une fois les modalités d'accès aux données communiquées, l'utilisateur pourra par ailleurs nous demander de partager les données facilement accessibles et les métadonnées auxquelles il a accès en vertu du Règlement avec un tiers éligible. Le tiers aura également accès aux données sans retard injustifié, à un niveau de qualité identique à celui dont bénéficie Renault, de manière aisée, sécurisée et dans un format complet, structuré, couramment utilisé et lisible par machine. Cependant, le tiers devra le cas échéant s'acquitter d'une compensation financière envers Renault. (voir point 12).

À titre d'exemple, l'utilisateur pourra nous demander de partager, avec son garagiste ou sa compagnie d'assurance, les données facilement accessibles générées par son véhicule connecté.

La demande de l'utilisateur pourra viser tout tiers à l'exception des entreprises désignées comme « contrôleur d'accès » au sens du Règlement européen sur les marchés numériques, telles qu'Alphabet, Amazon, Apple, ByteDance, Meta et Microsoft.

Il est précisé que l'utilisateur ne peut pas partager avec des tiers les données facilement accessibles dans le cadre de l'essai de nouveaux produits connectés, substances ou procédés qui ne sont pas encore mis sur le marché à moins que leur utilisation par un tiers ne soit contractuellement autorisée.

8. Comment le tiers a-t-il accès aux données à la demande de l'utilisateur ?

Le tiers peut accéder aux données uniquement à la demande de l'utilisateur soit via API, soit via fichier JSON que l'utilisateur peut télécharger via un lien sécurisé.

Accès via API

1. Le tiers se rend dans la Section « Data Act » de la plateforme Mobilize Data Solutions pour consulter le catalogue des données disponibles.
2. Pour disposer des données, il crée un compte ou se connecte à son espace s'il dispose déjà d'un compte.
3. Il accepte les Conditions Générales de Vente et les Conditions Générales de Partage de Données.
4. Il accède à la documentation technique qui décrit les modalités de connexion aux API, et peut contacter Renault en cas de besoin via le formulaire dédié.
5. Une fois connecté aux API de Renault, il peut :

- vérifier si les données souhaitées sont disponibles pour le véhicule de l'utilisateur ;
- générer un lien sécurisé à partir duquel l'utilisateur pourra l'autoriser à accéder aux données,

6. L'utilisateur se connecte à son espace (MyRenault, MyDacia, MyAlpine, MyDuo) via le lien reçu et donne son autorisation.
7. Le tiers peut alors accéder aux données depuis l'API.
8. Une facture mensuelle est émise selon les modalités prévues dans les Conditions Générales de Vente.

Accès via Fichier (Format JSON)

Après autorisation confirmée par l'utilisateur, le tiers destinataire reçoit un courriel l'invitant à créer un compte sur la plateforme Mobilize Data Solutions afin d'accéder aux données désignées par l'utilisateur.

Avant d'accéder aux données, le tiers accepte les conditions générales de vente et les conditions générales de partage des données accessibles sur la plateforme Mobilize Data Solutions.

Le tiers reçoit un lien sécurisé par courriel lui permettant de télécharger les données concernées.

Les modalités de facturation et de paiement sont décrites dans les Conditions Générales de Vente des données.

9. Quelles sont les obligations des tiers recevant des données à la demande de l'utilisateur ?

Le tiers doit traiter les données uniquement aux fins et dans les conditions convenues avec l'utilisateur et dans le respect du droit de la protection des données personnelles.

Le tiers doit effacer les données qui ne sont plus nécessaires à la finalité convenue, sauf accord contraire avec l'utilisateur en ce qui concerne les données non personnelles.

Il est interdit aux tiers de :

- rendre l'exercice des choix ou des droits de l'utilisateur difficile, y compris en créant des choix biaisés, ou en contraignant, en trompant ou en manipulant l'utilisateur, ou en réduisant son autonomie, sa capacité de décision ou ses choix, y compris via une interface numérique ;

- utiliser les données qu'il reçoit à des fins de profilage, à moins que cela ne soit nécessaire pour fournir le service demandé par l'utilisateur et dans le respect du RGPD ;

- mettre les données qu'il reçoit à la disposition d'un autre tiers, à moins que cela soit prévu dans un contrat avec l'utilisateur, et à condition que l'autre tiers prenne toutes les mesures de protection nécessaires convenues entre le détenteur de données et le tiers pour préserver la confidentialité des secrets d'affaires ;

- mettre les données qu'il reçoit à disposition d'un contrôleur d'accès au sens du Règlement européen sur les marchés numériques ;

- utiliser ou partager les données qu'il reçoit pour développer un produit concurrençant le produit connecté dont proviennent les données auxquelles il a accès ;

- utiliser les données qu'il reçoit pour obtenir des informations sur la situation économique, les actifs ou les méthodes de production de Renault ou sur l'utilisation que nous en faisons ;

- avoir recours à des moyens coercitifs ou tirer avantage des éventuelles lacunes de l'infrastructure technique de Renault destinée à protéger les données pour obtenir l'accès aux données ;

- utiliser les données d'une manière qui nuit à la sécurité du produit connecté ou du service connexe ;

- enfreindre les mesures de protection des informations confidentielles et des secrets d'affaires convenues entre Renault ou le détenteur de secrets d'affaires et l'utilisateur;

- empêcher l'utilisateur qui est un consommateur de mettre à la disposition d'autres parties les données qu'il reçoit.

10. **Quelles mesures de protection peuvent être mises en œuvre en cas d'utilisation illicite des données ?**

Cas dans lesquels des mesures de protection peuvent être mises en œuvre	Mesures de protection pouvant être mises en œuvre
Lorsque le tiers ou le destinataire de données : - a fourni de fausses informations à Renault, a eu recours à des moyens trompeurs ou coercitifs ou a tiré avantage des éventuelles lacunes dans l'infrastructure technique de Renault destinée à protéger les données, aux fins d'obtenir des données ; - a utilisé les données mises à disposition à des fins non autorisées, y compris le développement d'un produit connecté concurrent ; - a divulgué illégalement des données à une autre partie ; - n'a pas maintenu les mesures techniques et organisationnelles	Le tiers ou le destinataire de données doit donner suite sans retard injustifié, à la demande de Renault ou du détenteur de secrets d'affaires ou de l'utilisateur : - d'effacer les données mises à disposition par Renault et les éventuelles copies de celles-ci ; - de mettre fin (i) à la production, à l'offre ou à la mise sur le marché ou à l'utilisation de biens, de données dérivées ou de services produits sur la base des connaissances obtenues grâce aux données mises à disposition par Renault, ou (ii) à l'importation, à l'exportation ou au stockage de biens non conformes destinés aux fins précitées ; - de détruire tout bien non conforme produit sur la base des connaissances

convenues avec Renault ou le détenteur de secrets d'affaires ; ou - a modifié ou supprimé des mesures techniques de protection appliquées par Renault afin d'empêcher l'accès non autorisé aux données, y compris les métadonnées, et de garantir le respect du Règlement, sans l'accord de Renault.	obtenues grâce aux données mises à disposition par Renault, lorsqu'il existe un risque grave que l'utilisation illicite de ces données cause un préjudice important à Renault, au détenteur de secrets d'affaires ou à l'utilisateur ou lorsqu'une telle mesure de destruction du bien non conforme ne serait pas disproportionnée au regard des intérêts de ces derniers ; - d'informer l'utilisateur de l'utilisation ou de la divulgation non autorisées des données et des mesures prises pour mettre fin à l'utilisation ou à la divulgation non autorisée des données ; - d'indemniser la partie lésée par l'utilisation abusive ou la divulgation de ces données auxquelles il a été accédé illégalement ou qui ont été utilisées illégalement.

Les mesures de protection énoncées ci-dessus s'appliquent également (i) à l'égard d'un utilisateur ou d'un destinataire de données lorsqu'il modifie ou retire des mesures techniques et organisationnelles de protection appliquées par Renault ou ne maintient pas de telles mesures prises par l'utilisateur en accord avec Renault ou, s'il ne s'agit pas de la même personne, par le détenteur de secrets d'affaires, afin de préserver les données protégées par les secrets d'affaires, (ii) ainsi qu'à l'égard de toute autre partie qui reçoit les données de l'utilisateur à la suite d'une infraction au Règlement.

L'utilisateur peut également utiliser les mesures de protection ci-dessus si un destinataire de données rend l'exercice de ses choix ou ses droits indûment difficile ou utilise les données qu'il reçoit à des fins de profilage, à moins que cela ne soit nécessaire pour fournir le service demandé par l'utilisateur.

11. Quelles sont les obligations des utilisateurs concernant les données ?

Les utilisateurs doivent :

- utiliser les données uniquement aux fins et dans les conditions convenues avec Renault et dans le respect des lois et règlements,

- respecter les mesures de protection convenues avec Renault pour préserver la confidentialité des données partagées,

- ne pas se servir des données obtenues auprès de Renault pour mettre au point un produit concurrençant le produit connecté dont proviennent les données, ni partager ces données avec un tiers dans cette intention,

- ne pas utiliser les données pour obtenir des informations sur la situation économique des actifs ou des méthodes de production de Renault,

- ne pas avoir recours à des moyens coercitifs ou tirer avantage des éventuelles lacunes dans l'infrastructure technique de Renault destinée à protéger les données, aux fins d'accéder aux données, et

- ne pas partager les données avec les tiers désignés comme « contrôleur d'accès » au sens du Règlement européen sur les marchés numériques.

12. **Quelles sont les obligations applicables à Renault en tant que détenteur de données vis-à-vis des destinataires de données ?**

Dans le cadre de relations entre entreprises, les modalités de mise à disposition des données entre Renault et les destinataires de données sont équitables, raisonnables, non discriminatoires et transparentes.

Renault s'abstient également de toute discrimination s'agissant des modalités de mise à disposition des données entre des catégories comparables de destinataires de données. Lorsqu'un destinataire considère que les conditions dans lesquelles des données ont été mises à sa disposition sont discriminatoires et formule une demande motivée en ce sens, Renault lui fournit, sans retard injustifié, des informations attestant l'absence de discrimination.

Renault n'adopte pas de clause contractuelle abusive au sens du Règlement et de clause qui, au détriment de l'utilisateur, exclut l'application des droits de l'utilisateur au titre du chapitre II du Règlement, y déroge ou en modifie les effets.

Renault ne met pas de données à la disposition d'un destinataire de données, y compris sur une base d'exclusivité, sauf si un utilisateur le demande au titre du chapitre II du Règlement.

Renault et les destinataires de données ne sont pas tenus de fournir des informations autres que celles qui sont nécessaires pour vérifier le respect des clauses contractuelles convenues pour la mise à disposition des données ou des obligations qui leur incombent au titre du droit de l'Union européenne et de la législation nationale adoptée conformément à ce droit.

Renault peut exiger une compensation de la part du destinataire de données pour la mise à disposition des données à la demande de l'utilisateur. Cette compensation sera non discriminatoire et raisonnable et pourra inclure une marge.

Cette compensation tient compte en particulier :

- des coûts occasionnés par la mise à disposition des données, dont, notamment, les coûts encourus pour le formatage des données, leur diffusion par voie électronique et leur stockage ;

- des investissements dans la collecte et la production de données, le cas échéant, en prenant en compte le fait que d'autres parties ont contribué ou non à l'obtention, à la production ou à la collecte des données en question ;

- du volume, du format et de la nature des données.

En revanche, lorsque le destinataire de données est une PME ou un organisme de recherche à but non lucratif et n'a pas d'entreprises partenaires ou liées qui ne sont pas considérées comme des PME, l'éventuelle compensation demandée par Renault ne peut excéder les coûts visés au premier tiret ci-dessus.

Renault fournira au destinataire de données des informations exposant la base de calcul de la compensation de manière suffisamment détaillée pour lui permettre d'évaluer si les exigences ci-dessus sont respectées.

13. Que faire en cas de contestation ?

En cas de réclamation, nous vous invitons à contacter Renault via le formulaire de demande d'information disponible dans la Section « Data Act » accessible via le footer du site web de la marque.

Nous nous efforcerons de répondre et de traiter votre demande dans les plus brefs délais.

Si toutefois vous n'êtes pas satisfait de notre réponse, vous pouvez saisir l'organe de règlement des litiges qui sera désigné à cet effet, sans préjudice de votre droit de demander réparation devant une juridiction française.

Cet organe est compétent pour les réclamations portant sur :

- les restrictions ou interdictions contractuelles relatives aux exigences de sécurité du produit connecté ou en cas de refus ou de suspension de partage de données pour protéger la confidentialité des données ;

- les modalités et conditions équitables, raisonnables et non discriminatoires applicables à la mise à disposition de données et à la façon de mettre ces données à disposition en toute transparence conformément aux chapitre III et IV du Règlement.

Version avril 2026