masternaut
A MICHELIN GROUP COMPANY

MASTERNAUT INSIGHTS

RGPD
Règlement Général sur la Protection des Données

Un point de vue d'expert

masternaut

A MICHELIN GROUP COMPANY

Avant-propos

Ces derniers mois, j'ai été approché par nombre de clients à la recherche d'informations concernant le règlement communautaire sur la protection des données (RGPD). La plupart ont exprimé le désir de comprendre les tenants et les aboutissants de cette réglementation ainsi que ses répercussions sur les données télématiques et leurs activités professionnelles.

Malgré les avis et les projections pessimistes qui circulent au sujet du RGPD, il s'agit avant tout d'une évolution majeure en matière de protection des données personnelles. Cependant, pour les entreprises conformes à la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le RGPD n'est qu'un prolongement des bonnes pratiques existantes.

Attention, cela ne veut pas dire qu'elles sont exemptes de changements profonds. Au contraire, le RGPD étend la portée de la protection des données et apporte des changements significatifs sur la façon dont les données personnelles sont définies et doivent être gérées par les organisations. Les gestionnaires de flotte doivent prendre conscience que le traitement et la gestion des données personnelles en leur possession, y compris celles qui sont issues de la télématique, sont soumises aux obligations du RGPD.

Ce document vise à répondre de manière précise et synthétique aux questions posées par les clients de Masternaut sur le RGPD. Il concerne le traitement des données personnelles dans un contexte de gestion de flotte.

J'espère qu'il vous sera utile.

Djamel Souici
Directeur Juridique Masternaut

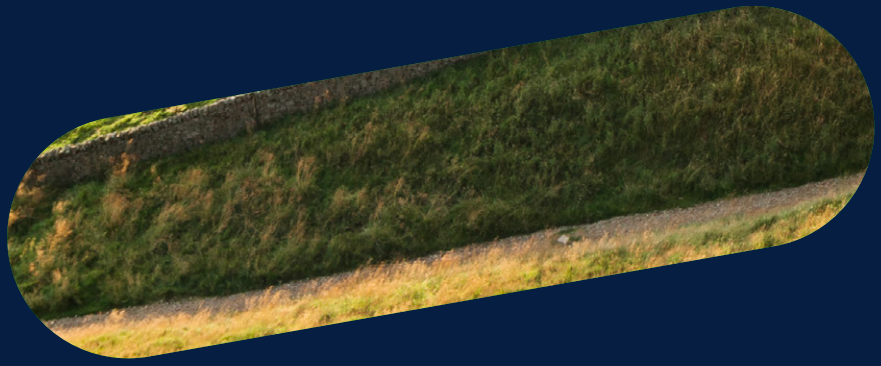
À propos de l'auteur

Djamel Souici est le Directeur Juridique de Masternaut. Son équipe est composée de spécialistes juridiques paneuropéens qui s'appuie également d'un réseau de cabinet d'avocats pour soutenir les activités de Masternaut en Europe.

Djamel fournit des conseils d'expert dans les domaines de la gouvernance d'entreprise, de la conformité, du droit du travail, du contentieux, de la propriété intellectuelle et des transactions commerciales (fusions et acquisitions), ainsi que de la protection des données et de la vie privée.

Diplômé en droit de l'université de la Ruhr à Bochum, en Allemagne, Djamel a été admis au barreau avant de poursuivre une carrière en droit commercial. Avant de rejoindre Masternaut, Djamel a travaillé pour de grandes sociétés technologiques telles que Novell Corporation, et compte plus de 25 ans d'expérience dans le domaine de l'informatique.

Sommaire



Aperçu

Le **Règlement Européen sur la Protection des Données (RGPD)** est entré en vigueur le 25 mai 2018.
Son objectif est d'harmoniser les lois sur la confidentialité des données en Europe afin de protéger les données personnelles des citoyens des États membres de l'Union européenne (UE). Avant, les législations sur la protection des données n'étaient pas toutes adaptées aux nouvelles évolutions du numérique. Pour les gestionnaires de flotte, plusieurs facteurs doivent être pris pour une gestion optimale de leur flotte dans le respect des obligations.

Le responsable du traitement des données et le sous-traitant

Le RGPD ne modifie pas les définitions des termes : « Responsable du traitement des données » et « Sous-traitant ». Il convient de faire un rappel de chacun de ces rôles

- Le **Sous-traitant** est l'organisation qui traite les données personnelles pour le compte du responsable du traitement des données. Cette définition comprend tous les prestataires délivrant des services en ligne de type « Cloud » tel que Masternaut.
- Le **Responsable du traitement des données** reste défini comme l'organisation qui « seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement » des données personnelles. **Les clients de Masternaut appartiennent à cette catégorie**.

Il est important de noter que Masternaut ne définit pas la finalité du traitement des données personnelles.

Celle-ci relève de la responsabilité du client en tant que Responsable du traitement des données personnelles.

Application du RPGD

Le RGPD s'applique lorsque le Responsable du traitement des données ou le sous-traitant ou la personne physique concernée est basé dans l'Union Européenne.
Le Règlement s'applique aussi aux organisations établies en dehors de l'UE lorsqu'elles collectent ou traitent des données à caractère personnel en relation avec les résidents de l'UE.

Dans le cadre du processus d'harmonisation, un seul ensemble de règles aujourd'hui s'applique à tous les États membres de l'UE. Pour les organisations qui disposent de plusieurs établissements en Europe, celle-ci doivent se justifier auprès l'autorité de l'État dans lequel se situe leur établissement principal (maison mère).

Avant le RGPD, la gestion du respect des règles était plus complexe. Une organisation avec plusieurs établissements en Europe était responsable devant les autorités de protection des données de chaque pays dans lequel elle exerce son activité. Les lois nationales devaient être aussi appliquées.

En France, l'autorité de protection des données personnelles est la CNIL (Commission Nationale Informatique et Libertés).

Que retenir ?

Depuis le 25 mai 2018, le RGPD permet aux entreprises d'être responsable devant une seule autorité de protection des données. Cela a été rendu possible car le RGPD n'est pas une directive de l'UE, mais un Règlement (UE2016/679).

Données personnelles et gestion de flotte

Les gestionnaires de flotte doivent tenir compte des obligations imposées par le RGPD. Dans le cadre de leur activité, ceux-ci ont accès, traitent et gèrent généralement toutes les informations relatives aux conducteurs. Ces informations sont considérées comme étant des données personnelles.

Les « données personnelles » désignent les données liées à une personne physique identifiée ou identifiable (la « personne concernée »). Pour les gestionnaires de flotte, il s'agit plus généralement des «conducteurs ».

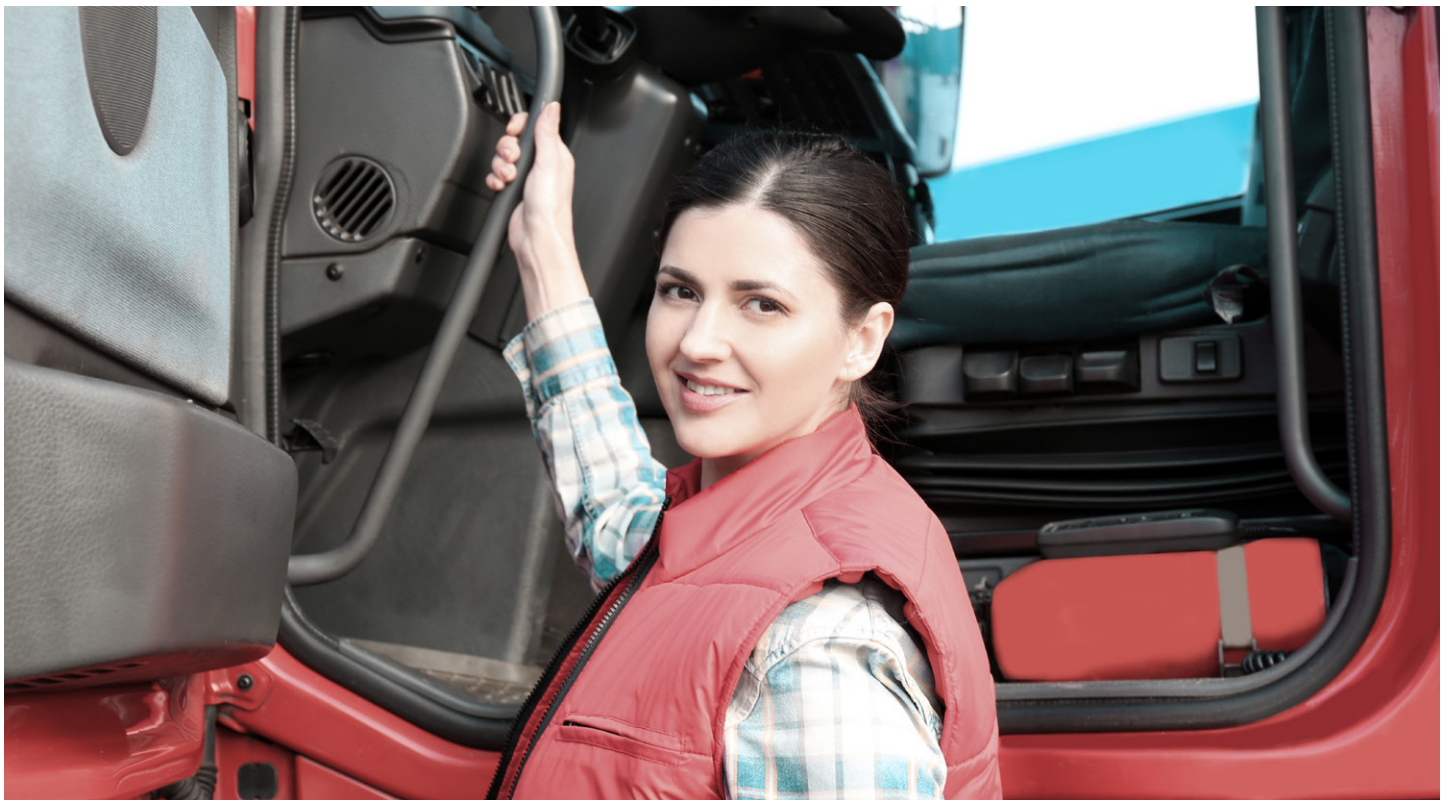
Une personne concernée par le RGPD est directement identifiable à partir des données qui lui sont attachées et indirectement à travers une référence (un nom, un numéro d'identification, des données de localisation, un identifiant numérique...) ou d'autres éléments faisant référence à une personne physique.

Le RGPD apporte des changements importants et élargit la définition de "données personnelles" par rapport aux définitions précédentes. En outre, il permet d'étendre sa portée aux adresses IP des dispositifs utilisés par les conducteurs, leurs identifiants, numéros de téléphone, plaques d'immatriculation des véhicules... Les systèmes télématiques prenants en compte certains identifiants pouvant être liés aux conducteurs sont tout aussi concernés.

Le RGPD exige que les données personnelles soient :

- Traitées de manière **licite, loyale et transparente,**
- Recueillies à **des fins déterminées, explicites et légitimes** et non traitées de manière incompatible avec ces finalités,
- **Adéquates, pertinentes et limitées** à ce qui est nécessaire pour atteindre ces objectifs,
- **Exactes** et **tenues à jour**,
- **Conservées pendant une durée n'excédant pas celle qui est nécessaire** pour atteindre les objectifs pour lesquels elles ont été recueillies,
- Correctement **sécurisées** contre la perte accidentelle, la destruction ou les dommages.

Le RGPD impose d'autres obligations aux organisations. Par exemple, la nécessité de documenter leurs activités de traitement et d'être en mesure de **démontrer leur conformité** aux principes cités ci-dessus.



Cadre légale du traitement des données personnelles

Après avoir établi un processus de gestion des données, il convient de s'assurer de l'existence d'une base légale (qui devra être documentée) pour le traitement. Dans le cadre du RGPD, cette partie est très importante car la définition d'une base légale de traitement a un effet sur les droits des individus. Par exemple, un traitement des données personnelles basé sur le consentement confère généralement des droits plus importants à l'individu concerné, tels que le droit de faire effacer ses données.

Il existe des options autre que le consentement pour un traitement légal des données. En effet, le traitement est légal s'il est :

- Avoir obtenu le consentement préalable des personnes concernées, qui doit être éclairé et exprès,
- Poursuivre un intérêt légitime,
- S'inscrire dans le cadre des nécessités engendrées par l'exécution d'un contrat,
- Un traitement à réaliser dans l'intérêt public ou dans l'exercice de l'autorité publique,
- Un traitement imposé par une obligation légale,
- Protéger les intérêts vitaux des personnes concernées.

Nous vous conseillons de choisir judicieusement votre base légale car les droits des personnes concernées peuvent varier.

Consentement

Le consentement du conducteur n'est pas nécessaire si, par exemple, les données sont utilisées à des fins de gestion de la paie.

Si un employé est rémunéré pour le temps de conduite et que des données télématiques sont utilisées pour enregistrer ses heures, le traitement est couvert par le contrat de travail. Une telle utilisation relève de l'exception de traitement pour l'exécution d'un contrat et le consentement du conducteur n'est pas requis.

Lorsqu'une autorisation de traitement s'appuie sur des intérêts légitimes, les gestionnaires de flotte doivent veiller à ce que l'équilibre entre leurs intérêts et celui des conducteurs soit dûment documenté. Ils doivent, en effet, prendre en compte que les conducteurs ont pour attente un traitement de leurs données basé sur vos intérêts légitimes ; incluant ainsi la prévention contre la fraude, la sécurité des données et des conducteurs, etc.

En l'absence de base contractuelle ou d'intérêt légitime, les gestionnaires de flotte doivent demander le consentement du conducteur. Ce consentement doit être spécifique, faire absence d'ambiguïtés et doit être donné librement.

Les objectifs doivent être clairs afin que les conducteurs sachent dès le départ quelles informations sont recueillies, pourquoi elles le sont et ce qu'il advient de ces informations, y compris des détails sur les personnes/parties avec qui elles seront partagées. Les raisons doivent être simples. Par exemple, « pour mesurer, gérer, et réduire la consommation de carburant et les émissions de CO2 » est une raison parfaitement légitime. Par contre, mesurer les survitesses n'est probablement pas un objectif permis.

Le consentement doit être documenté et idéalement incorporé dans les contrats de travail, du fournisseur et du conducteur, ainsi que dans les conditions générales d'achat. Parvenir au consentement dans ces procédures devrait réduire le risque de conflits futurs.

Protection des données dès la conception et par défaut (Privacy by design et Privacy by default)

Avec le RGPD, les gestionnaires de flotte ont pour obligation de mettre en œuvre des mesures techniques et organisationnelles pour montrer que la protection des données a été intégrée dans les activités commerciales ainsi que dans les activités de traitement des données.

Ce sont des mesures qui devront respecter les principes de "protection des données dès la conception" et "protection des données par défaut » ; en anglais Privacy by design et Privacy by default.

Qu'est-ce que cela signifie ?

Les mesures de protection des données doivent être intégrées dès le développement des processus commerciaux afin de limiter le traitement pour ce qui est nécessaire ; c'est-à-dire faire correspondre le traitement aux raisons pour lesquelles les données ont été recueillies. Il s'agit également de limiter les accès aux données personnelles aux bonnes personnes de l'organisation.

La protection des données dès la conception et par défaut comprend aussi l'obligation de concevoir des processus afin que les mesures prises pour améliorer la protection de la vie privée (exemple : pseudonymisation des données à caractère personnel) soient mises en place par le responsable du traitement des données dès que possible.

Le registre des activités de traitement

Les gestionnaires de flotte doivent fournir des politiques de confidentialité complètes, claires et transparentes. Dans le cas où votre organisation dispose de 250 employés ou plus, il est nécessaire de tenir des rapports internes des activités de traitement.

Ces rapports doivent contenir les informations suivantes :

- Le nom et les coordonnées du **responsable du traitement des données** et du délégué à la protection des données,
- La finalité, c'est-à-dire le but du traitement,
- Une description des **catégories de personnes concernées** et des **catégories de données personnelles**,
- La ou les catégories de destinataires des données personnelles,
- Indiquer si les données personnelles sont transférées vers des pays tiers ou des organisations internationales,
- Les durées de **conservation** des données par catégorie de données,
- « Dans la mesure du possible », une description générale des mesures techniques et organisationnelles de sécurité mises en place pour protéger et sécuriser les données personnelles.

Les rapports doivent être écrits (mais peuvent être sauvegardés sous forme électronique) et doivent être disponibles sur demande de l'autorité de protection des données compétente.

Délégué à la Protection des données (ou "DPO", en anglais pour "Data Protection Officer")

En vertu du RGPD, un responsable de la protection des données doit être nommé par une organisation si les circonstances suivantes sont remplies :

- L'organisation est une autorité publique (à l'exception des tribunaux agissant dans leur capacité judiciaire),

OU

- Un suivi systématique à grande échelle des individus (par exemple, le suivi du comportement en ligne ou des conducteurs dans les grandes flottes) doit être effectué,

OU

- Le traitement à grande échelle de catégories spéciales de données.

Le rôle du responsable de la protection des données est le suivant :

- Informer et conseiller l'organisation et ses employés sur leurs obligations de se conformer au RGPD et à d'autres lois relatives à la protection des données,
- Surveiller le respect du RGPD et d'autres lois relatives à la protection des données, y compris la gestion des activités internes de protection des données, le conseil sur les DPIA, la formation du personnel et la conduite d'audits internes,
- Être le premier point de contact pour les autorités de surveillance et pour les personnes dont les données sont traitées (employés, clients, etc.),
- Signaler, le cas échéant, les violations de données aux autorités de surveillance.

Si une organisation nomme un responsable de la protection des données, l'individu en poste doit :

- Faire rapport au plus haut niveau de gestion de l'organisation, c'est-à-dire au niveau du conseil,
- Opérer de manière indépendante et ne pas être licencié ou pénalisé pour avoir accompli sa tâche,
- Disposer des ressources adéquates pour remplir ses obligations relatives au RGPD.

Un salarié peut se voir confier le rôle de responsable de la protection des données dans la mesure où ses fonctions actuelles sont compatibles avec les devoirs du responsable de la protection des données et n'entraînent pas de conflit d'intérêts. Le rôle peut également être externalisé.

Bien que le RGPD ne spécifie pas les qualifications précises qu'un agent de la protection des données est censé posséder, il exige qu'il ait une expérience professionnelle et une connaissance de la loi sur la protection des données. Cela doit être proportionnel au type de traitement effectué par l'organisation, en tenant compte du niveau de protection requis par les données personnelles.

© 2018 Masternaut

Transferts de données en dehors de l'UE

La plupart des gestionnaires de flotte font usage de la télématique par le biais d'organismes tiers qui traitent les données télématiques en prenant ainsi la casquette du responsable du traitement des données. Néanmoins, cela n'exonère pas le gestionnaire de flotte de sa responsabilité d'assurer un traitement légal des données.

C'est le cas, par exemple, des données transférées à l'étranger. Les données des citoyens de l'UE peuvent être traitées partout au sein de l'UE. Mais, le **RGPD restreint les possibilités de traitement hors de l'UE**. Ces restrictions sont similaires à celles qui sont fixées par la directive 95/46/CE, mais avec un cadre plus complexe de règles et d'exceptions.

Les gestionnaires de flotte doivent s'assurer du traitement licite des données personnelles. Pour les données télématiques de la flotte (susceptibles d'être considérées comme des données personnelles) qui ne sont pas traitées dans l'UE, les gestionnaires de flotte doivent veiller à ce que les conditions du RGPD qui permettent le transfert de données à caractère personnel en dehors de l'UE soient respectées.

Si vous ne respectez pas les règles relatives aux transferts en tant que responsable du traitement des données, vous pouvez être poursuivi par les autorités compétentes. Dans le cas où l'infraction n'est pas corrigée conformément aux exigences de ces autorités, vous êtes passible de lourdes amendes.

En règle générale, les transferts de données personnelles vers des pays tiers (États non membres de l'UE) ou vers des organisations internationales ne peuvent être effectués que si le responsable du traitement des données et son sous-traitant ont pleinement respecté les dispositions du RGPD.

Il convient également de noter que tout transfert de données personnelles effectué dans le cadre de la directive 95/46/CE reste valable dans le cadre du RGPD, sauf si la Commission européenne en décidait autrement. Cela signifie que les États qui figurent sur la **liste blanche**, c'est-à-dire ceux qui fournissent le même niveau de protection des données personnelles que l'UE, restent des territoires vers lesquels les données personnelles peuvent être transférées et traitées sans le consentement des personnes concernées ou de l'autorité de protection des données.

La Suisse est un exemple de pays inscrit sur la liste blanche. Par contre, **les États-Unis ne figurent pas sur la liste blanche**.

Les pays qui figurent sur la liste blanche font l'objet d'un suivi permanent de la part de la Commission européenne. Ils peuvent être susceptibles d'être retirés de la liste si le niveau de protection des données personnelles ne correspondait pas aux attentes et aux normes requises en Europe.

Si des données personnelles doivent être traitées dans des pays ne figurant pas sur la liste blanche, le RGPD exige que des garanties appropriées soient accordées, telles que l'insertion, dans les contrats, de clauses standards de protection des données adoptées par la Commission européenne ou, approuvées par la Commission européenne, lorsqu'elles émanent des autorités de protection des données.

L'UE n'a pas encore publié de clauses standards dans le cadre du RGPD, mais elle a indiqué que ses clauses-types prévues pour le traitement des données effectuées dans le cadre de la directive 95/46/CE restent valables jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées.

Cela est très important pour les transferts de données vers des pays tiers et, en particulier, vers les États-Unis. Il s'agit, en effet, de garantir une base légale pour le transfert des données lorsque le RGPD entrera en vigueur.

Les gestionnaires de flottes doivent donc vérifier en permanence la validité de leurs contrats avec les entreprises auxquelles ils sous-traitent le traitement de leurs données personnelles. En cas de contrat non-conforme, le gestionnaire de flotte s'expose à des sanctions administratives et est passible de lourdes amendes.

Le consentement des personnes concernées reste une base appropriée pour un traitement licite des données en dehors de l'UE. Toutefois, le RGPD indique clairement que toutes les personnes concernées doivent consentir « explicitement » au transfert de leurs données personnelles après avoir été informées des risques éventuels de transfert.

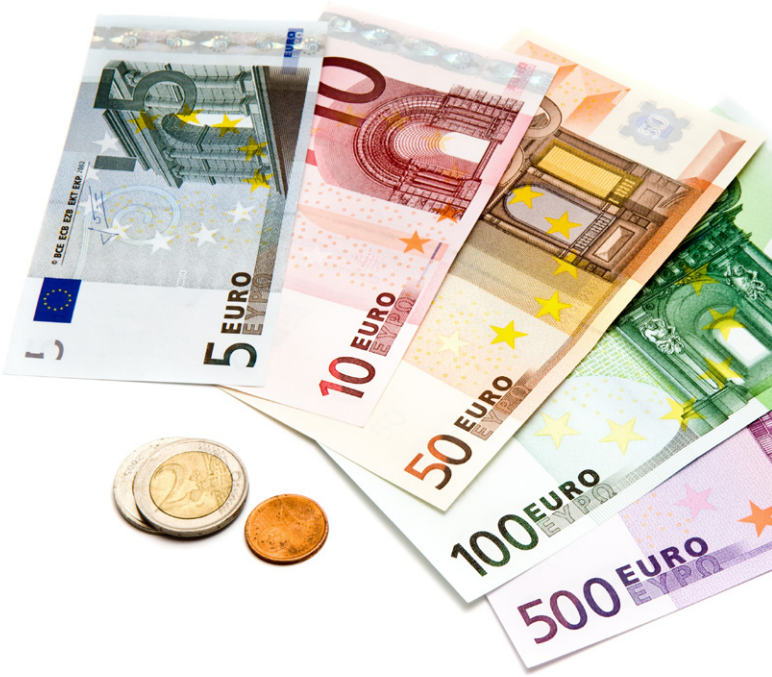
Que retenir ?

Le RGPD instaure un cadre réglementé et contrôlé pour les transferts de données vers des pays tiers ou des organisations internationales. En tant que gestionnaire de flotte, pour éviter les risques d'amendes et les contrats complexes, il est préférable que votre prestataire de services de télématiques vous confirme que ses traitements sont réalisées au sein de l'UE.

Les sanctions

Les lois nationales sur la protection des données personnelles ont souvent été perçues comme des lois très strictes. Pourtant, les sanctions qu'elles prévoyaient étaient faibles pour les responsables de traitements et les sous-traitants.

Le RGPD change la donne. Le montant des amendes peut aller, selon la catégorie d'infraction, **jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial consolidé d'une entreprise** pour les infractions les plus graves. Les amendes sont susceptibles d'être importantes en cas de violation grave des principes de traitement des données personnelles. Cela comprend le consentement de la personne concernée et les transferts illégaux de données personnelles dans des pays tiers.

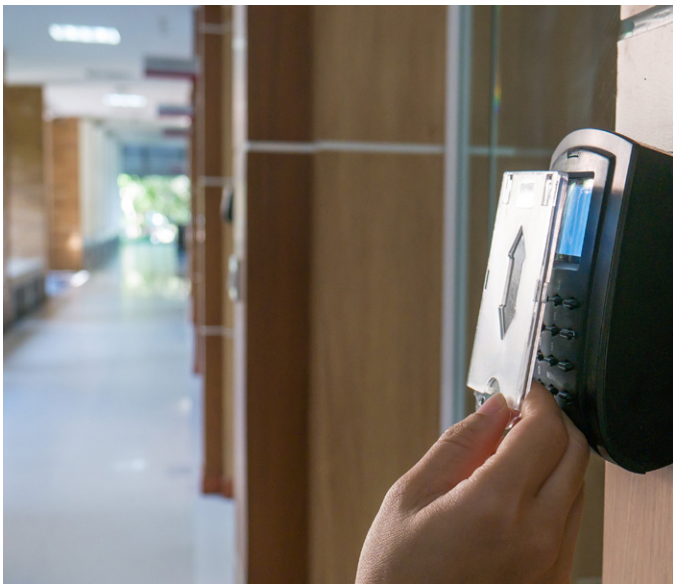


Masternaut et le RGPD

Garantir la sûreté et la sécurité des données de nos clients constitue notre principale priorité. Au cours des dernières années, nous avons réalisé d'importants investissements dans la protection et la sécurité des données. Par conséquent, Masternaut sera prête et satisfera les exigences du RGPD avant l'échéance.

Nous avons, en effet, une longue expérience dans le traitement des données. En outre, nous avons développé des processus organisationnels et des mesures de sécurité qui correspondent ou dépassent les exigences de la loi de 1978 et de la directive européenne 95/46/CE.

Nous avons pris ces mesures supplémentaires afin d'assurer la sécurité et la sûreté des données clients en notre possession, et répondre aux exigences du RGPD.



Certification ISO27001

Masternaut est officiellement certifiée ISO 27001:2017.

ISO 27001 (également connue sous le nom ISO/IEC 27001:2005) est une norme internationale de système de gestion de la sécurité de l'information (ISMS).

Qu'est-ce que cela signifie ?

Il s'agit d'un ensemble de politiques et de procédures ayant pour objet de protéger les fonctions et les informations de toutes pertes (vol ou altération) et les systèmes informatiques, de toutes intrusions et sinistres.

La norme ISO27001 inclut tous les contrôles juridiques, physiques et techniques qui concernent les processus de gestion des risques afférents aux données d'une organisation.

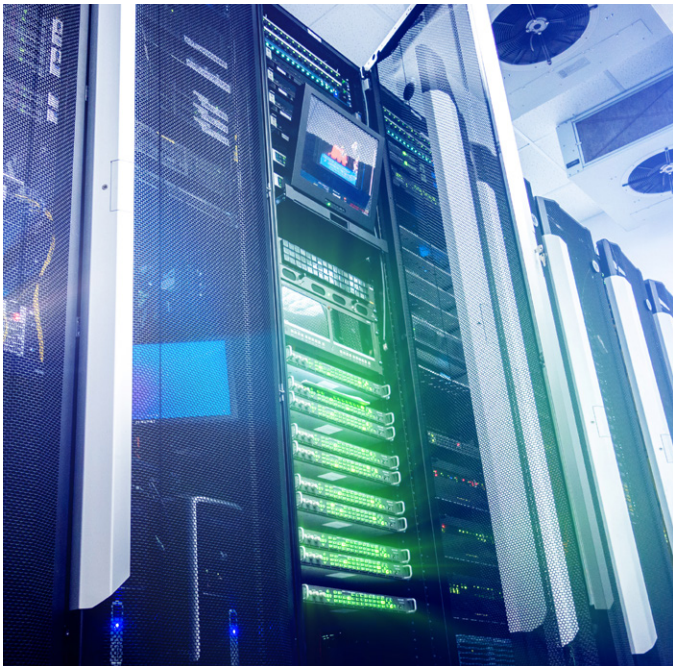
Selon le RGPD, les données personnelles sont des informations critiques que toutes les organisations doivent protéger. La certification ISO27001 permet à nos clients de confirmer la confiance qu'ils attendent de Masternaut en matière de protection de leurs données personnelles.

THE BRITISH ASSESSMENT BUREAU
ISO27001
Certification No. 214521

Bien entendu, certaines exigences du RGPD de l'UE ne sont pas directement couvertes par la norme ISO 27001. Par exemple, la prise en charge des droits des personnes concernées, c'est-à-dire le droit d'être informé, de voir ses données supprimées ou la portabilité des données personnelles. Toutefois, étant donné que la mise en œuvre de la norme ISO27001 identifie les données personnelles comme étant des éléments essentiels de la sécurité de l'information, la plupart des exigences du RGPD sont couvertes par défaut.

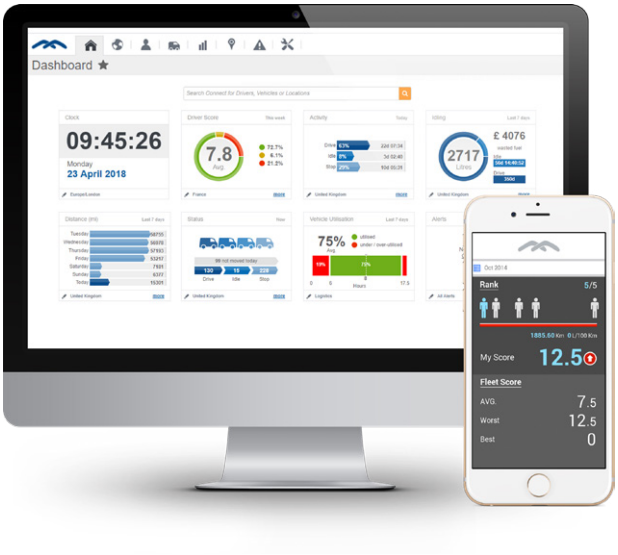
Centres de données

Les données télématiques de nos clients sont actuellement traitées exclusivement dans nos propres centres de données, en France et au Royaume-Uni. Aucune donnée personnelle n'est transmise à un prestataire de cloud tiers ou n'est hébergée dans un centre de données partagé. Nos centres de données sont sécurisés par une gamme de logiciels de cybersécurité complète et testée de manière indépendante. Les contrôles d'accès physiques et biométriques garantissent que seuls les employés autorisés y ont accès.



Respect de la vie privée dès la conception

La principale plateforme télématique de Masternaut, **Masternaut Connect**, prend en compte la notion de confidentialité dès sa conception.



Dans Connect, le modèle d'accès basé sur les rôles permet aux administrateurs de paramétrer des droits d'accès et de définir des rôles pour chaque utilisateur. À cet effet, les administrateurs ont la possibilité de contrôler tous les accès ainsi que de les limiter en fonction de la typologie d'utilisateurs présents sur la plateforme.

Accès aux données et portabilité des donnée

Masternaut a mis en place des processus et des infrastructures permettant de traiter toutes les requêtes du responsable du traitement et de favoriser la coopération avec celui-ci. Toutes les données personnelles sur la plate-forme Connect sont portables et, suivant l'habilitation, peuvent être téléchargées par le client et réutilisées.

Les données de télématiques sont uniquement traitées dans les centres de données de Masternaut au Royaume-Uni ou en France. Des mesures ont été mises en place afin de s'assurer que seuls les employés habilités ont accès aux données des clients. Ils ont été **nommés délégués à la protection des données pour nos data centres**.

L'analyse d'impact relative à la protection des données (DPIA : Data Protection Impact Assessment)

Une évaluation générale des risques pour tous les actifs informationnels gérés par Masternaut a été réalisée dans le cadre de la procédure de certification ISO27001. En vertu de l'article 35 du RGPD, une analyse d'impact est exigée des responsables du traitement lorsque le traitement est effectuée au moyen des nouvelles technologies, ce qui peut entraîner un risque élevé pour les droits et les libertés des personnes physiques.

Étant donné que Masternaut est le sous-traitant des données de ses clients et qu'aucune des données collectées par nos soins ou stockées sur la plate-forme Connect ne remplit les critères ci-dessus, nous ne sommes pas tenus de réaliser une analyse d'impact.

Cette obligation relève de la responsabilité du client en tant que responsable du traitement. Dans le cas où le client n'utilise pas les données comme mentionné à l'article 35, il n'est pas nécessaire d'envisager une analyse d'impact.

Résumé

Certaines exigences de mise en conformité du RGPD peuvent sembler difficiles à satisfaire pour les entreprises. Cependant, une grande partie d'entre elles ne constitue qu'un prolongement de la législation en vigueur. Une majorité de nos clients n'auront pas besoin de réaliser des modifications importantes.

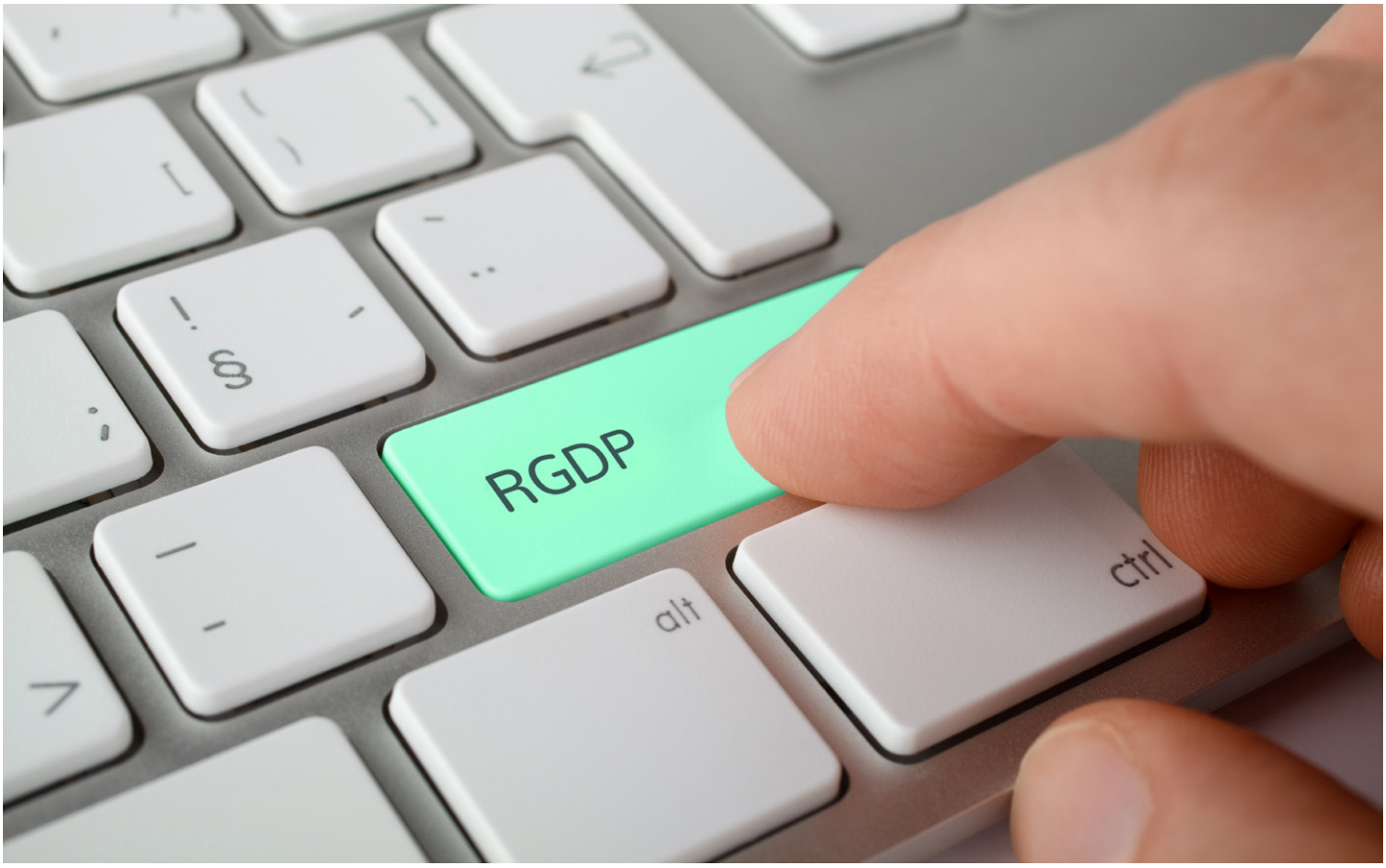
Le respect des obligations imposées par le RGPD n'est pas facultatif et il existe des niveaux de complexité qui ne sont pas nécessairement apparents. Les gestionnaires de flotte sont informés des pénalités et des amendes existantes et doivent prendre toutes les mesures nécessaires pour se conformer à la nouvelle réglementation afin de réduire leurs risques.

C'est une recommandation évidente, mais une consultation auprès de vos conseillers juridiques (juristes internes ou avocats) est la meilleure recommandation à suivre en amont d'un chantier RGPD, d'autant plus qu'ils ne peuvent pas connaître a priori la quantité et le contenu des données qui sont gérées et dont disposent les gestionnaires de flotte.

La CNIL fournit également d'excellentes explications ainsi que des outils utiles pour garantir la protection des données : https://www.cnil.fr/fr/comprendre-le-reglement-europeen

Avertissement

Veuillez noter que toutes les interprétations du RGPD qui figurent dans ce document sont adaptées aux faits et au contexte. Les informations contenues dans ce document ne doivent pas être considérées comme étant des conseils juridiques et ne peuvent être invoquées pour déterminer comment le RGPD s'applique à votre organisation. Nous vous encourageons à vous rapprocher de votre conseiller juridique pour connaître la manière dont le RGPD s'applique spécifiquement à votre entreprise. Ces informations sont fournies « telles quelles » et peuvent être mises à jour ou modifiées sans préavis. Le contenu de ce document peut être référencé ou copié et utilisé à des fins de référence internes uniquement.



masternaut

A MICHELIN GROUP COMPANY

À PROPOS DE MASTERNAUT

Chez Masternaut, filiale à 100% du groupe Michelin, notre objectif est de fournir une mobilité durable grâce à la connectivité. En tant que l'un des plus importants fournisseurs de services de télématique en Europe, avec des positions de leader au Royaume-Uni et en France, nous fournissons aux entreprises des solutions connectées pour le suivi et l'optimisation de leur flotte, la gestion des processus de missions, la sécurité et l'amélioration du comportement des conducteurs, ainsi que la réduction des émissions de CO_2.

Plus d'informations :
www.masternaut.com

masternaut
*A **MICHELIN** GROUP COMPANY*

Paris | Londres | Leeds | Rouen
Masternaut | Tour W - 102 Terrasse Boieldieu | 92800 Puteaux | France
T. +33 2 32 25 37 00 E. info@masternaut.com
www.masternaut.fr