TOMTOM
TELEMATICS

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

« L'afflux important de données de flotte s'est accompagné d'inquiétudes quant à la sécurité et la confidentialité de ces données »

L'utilisation et le flux de données relatifs à l'activité de leur flotte sont devenus des enjeux importants pour les entreprises. En effet, celles-ci souhaitent s'assurer de la sécurité et de l'efficacité de leur activité.

L'afflux important de données de flotte, largement lié à la télématique, s'est cependant accompagné d'inquiétudes quant à la sécurité et la confidentialité de ces données. L'entrée en vigueur du Règlement Général européen sur la Protection des Données (RGPD) met la priorité sur ces enjeux.

La majeure partie des exigences du RGPD est déjà couverte par la législation. De ce fait, les organisations déjà en conformité et ayant mis en place des meilleures pratiques peuvent selon nous considérer le RGPD comme la continuité de leurs activités.

Les gestionnaires de flotte et les acteurs de leur chaîne logistique doivent s'assurer qu'ils disposent d'une infrastructure, de procédures et d'une culture adéquates afin de respecter le RGPD. Les conséquences d'une violation des exigences peuvent être graves. Lors du développement de ses solutions, TomTom Telematics accorde beaucoup d'importance au RGPD, qui est également au centre des conseils et de l'assistance que nous proposons à nos clients.

Dans ce document, nous allons expliquer ce que cette nouvelle réglementation peut avoir comme conséquences pour votre entreprise et votre flotte. Nous vous proposerons des conseils pratiques qui vous aideront à rester en conformité avec la loi.

Thomas Schmidt,
Directeur général, TomTom Telematics

CLAUSE DE NON-RESPONSABILITÉ : les informations figurant dans la documentation TomTom Telematics et en ligne sont fournies à titre informatif uniquement et expriment notre opinion sur le sujet abordé. Elles ne sauraient constituer un conseil juridique sur le sujet. En outre, les informations contenues dans ces documents et en ligne pourraient ne pas refléter l'évolution des exigences juridiques. Vous ne devez pas agir en vous appuyant sur ces informations sans obtenir au préalable un avis juridique.

LE RGPD : PRÉSENTATION

Notre monde numérique est aujourd'hui très différent de ce qu'il était lorsque la Directive européenne sur la protection des données personnelles est entrée en vigueur en 1995.

Bien que ses principes généraux demeurent valables, la législation a été mise à jour avec l'introduction du Règlement Général sur la Protection des Données (RGPD). Le RGPD, qui entrera en vigueur le 25 mai 2018, vise à harmoniser les lois relatives à la confidentialité des données dans toute l'Europe, afin de protéger de manière adéquate l'ensemble des citoyens européens.

Il se concentre essentiellement sur la protection des données personnelles, définies comme « toute information ou données qui peuvent ou pourraient être liées à une personne identifiable ». Le RGPD fait donc l'objet de nombreuses préoccupations de la part des gestionnaires de flotte, qui doivent souvent accéder ou gérer les données des conducteurs.

Ces nouvelles règles ne sauraient constituer une révision complète de la législation sur la protection des données. Elles doivent plutôt être considérées comme une extension des réglementations existantes et des meilleures pratiques actuellement adoptées par les entreprises.

> Le RGPD harmonise la législation en matière de confidentialité des données en Europe, afin de s'assurer que tous les citoyens européens sont protégés de manière adéquate

EN QUOI LE RGPD A-T-IL UN IMPACT SUR LA PROTECTION DES DONNÉES DANS LE SECTEUR DES SOLUTIONS TÉLÉMATIQUES ?

Le RGPD apporte plusieurs modifications importantes aux lois relatives à la confidentialité des données, qui pourraient avoir des conséquences sur la gestion de flotte et l'utilisation des solutions télématiques.

1 **L'individu occupe une place centrale.** Au cœur du RGPD figure la responsabilisation des personnes, qui doivent donc être informées à l'avance des données utilisées, de l'objectif dans lequel elles sont utilisées, de la durée de leur utilisation et de qui les utilise. Chacun peut donner ou non son autorisation et, dans une certaine mesure, demander à ce que ses données personnelles ne soient plus utilisées.

2 **Une évaluation des risques et une piste d'audit sont indispensables.** Lorsqu'elles exploitent des données personnelles, les entreprises doivent identifier et limiter les risques de mauvaise utilisation des données, mais aussi mettre en place une documentation indiquant comment les données sont utilisées et comment assurer la conformité de leur traitement.

3 **Certaines entreprises doivent également nommer un délégué à la protection des données (DPO).** Le RGPD impose aux entreprises menant à bien certains types d'activités de traitement de nommer un délégué à la protection des données (ou DPO, Data Protection Officer), par exemple, lorsque leurs activités principales impliquent la surveillance systématique des personnes à grande échelle. Plus d'informations dans ce guide.

4 **Les entreprises ont un régulateur unique comme point de contact.** Les entreprises actives dans plusieurs pays européens, notamment celles dont les véhicules traversent les frontières, sont désormais régies par un ensemble de lois unique et traitent avec un seul régulateur : celui du pays dans lequel se situe leur siège social.

5 **Des exigences de sécurité plus strictes.** Les données personnelles sont désormais protégées contre toute sorte d'utilisation non autorisée, et ce en fonction de la sensibilité des données. Les données de localisation GPS fournies par un système télématique peuvent constituer des données sensibles, car elles en disent long sur la personne concernée.

6 **Des amendes plus élevées en cas de non-conformité.** Le RGPD stipule que l'amende maximale en cas d'infraction est de 20 millions d'euros, ou 4 % du chiffre d'affaires, le montant le plus élevé étant retenu.

QUELS SONT LES RÔLES DÉFINIS PAR LE RGPD ?

Les personnes en charge du contrôle et du traitement des données sont soumises au RGPD. Dans la plupart des cas, les entreprises jouent le rôle de contrôleur des données, tandis que le traitement des données est assuré par leurs sous-traitants. Néanmoins, ces deux rôles sont définis comme suit :

- Un **sous-traitant** (« data processor ») est une organisation qui traite les données personnelles au nom d'un contrôleur. TomTom Telematics joue le rôle de sous-traitant pour toutes les données personnelles fournies par ses clients et partenaires via ses systèmes et plateformes.

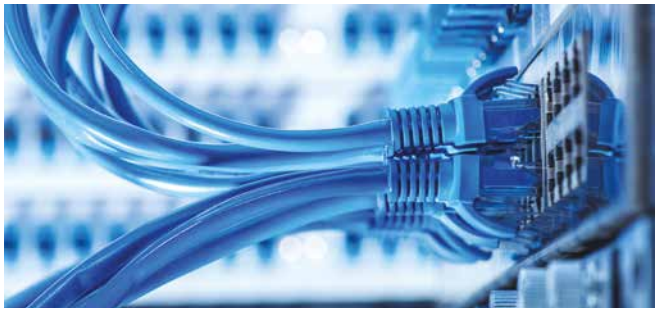
- Un **contrôleur des données** est une organisation qui détermine à quelles fins et selon quelles méthodes les données personnelles sont traitées. Par exemple, pour les données de flotte fournies par notre solution de gestion de flotte SaaS (Software-as-a-Service) WEBFLEET, l'entreprise agit en tant que contrôleur des données dans la mesure où elle décide comment les données sont utilisées (notamment pour aider à assurer la sécurité de ses employés sur la route).

L'une des principales modifications apportées aux réglementations relatives à la protection des données par le RGPD est que les sous-traitants devront à présent également se conformer aux réglementations, alors qu'auparavant, cette responsabilité incombait uniquement aux contrôleurs.

QUELLES SONT LEURS RESPONSABILITÉS ?

Les principales responsabilités des organisations sont définies dans les principes de protection des données du RGPD, qui stipulent que les données personnelles doivent être :

- traitées dans le respect de la loi, de manière juste et transparente ;
- recueillies à des fins précises, claires et légitimes, et ne doivent pas être traitées de manière incompatible avec ces fins ;
- adéquates, pertinentes et limitées au strict nécessaire en vue d'atteindre les objectifs pour lesquels elles sont traitées ;
- précises et, si nécessaire, mises à jour régulièrement ; tout le nécessaire doit être fait pour s'assurer que les données personnelles erronées soient effacées ou rectifiées dès que possible ;
- conservées sous une forme qui permette l'identification de la personne concernée pour la durée strictement nécessaire en vue d'atteindre les objectifs pour lesquels elles sont traitées ;
- traitées de manière à s'assurer qu'elles demeurent adéquates et sécurisées.



QUELS TYPES DE DONNÉES PERSONNELLES SONT CONCERNÉS ?

Le RGPD précise et complète la définition de "données personnelles".

Un individu (ou « personne concernée ») peut être identifié directement ou indirectement. Les identifiants des données personnelles peuvent inclure toute information allant du nom d'un individu aux données associées à des identifiants uniques, telles que la plaque d'immatriculation ou le numéro d'identification d'un véhicule (VIN). Si la personne concernée peut être identifiée à partir des données (même si l'identification n'a pas lieu dans les faits), ces données sont considérées comme des données personnelles.

Les types de données personnelles liées à une personne identifiée ou identifiable peuvent inclure des avis, des faits, ainsi que tout autre élément allant des informations sur les performances aux supports de recrutement et aux notes prises lors des entretiens.

Une fois rendues anonymes, les données ne sont plus concernées par le RGPD si les procédures suivies ne permettent plus de les associer à une personne identifiable.

Un consentement explicite doit être donné pour tout partage de données personnelles sensibles : « données personnelles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ».

LES BASES JURIDIQUES EN MATIÈRE DE TRAITEMENT DES DONNÉES

Lorsque vous traitez des données personnelles, vous devez pouvoir vous appuyer sur un fondement juridique, et le motif de leur utilisation doit être prédéfini.

La justification la plus évidente demeure sans doute de disposer du consentement explicite de la personne dont vous traitez les données. Cependant, cela peut poser problème dans le cas des salariés, car il est difficile de faire valoir que le consentement a été donné librement.

C'est pourquoi il existe d'autres fondements juridiques pour le traitement des données. Quelle que soit l'option choisie, elle doit être clairement documentée.

- **Consentement :** dans ce cas, l'individu doit clairement consentir librement à ce que ses données soient traitées à une fin donnée. N'oubliez pas que ce consentement ne doit comporter aucune ambigüité, ne doit pas être présumé, et doit pouvoir être retiré à tout moment.
- **Intérêts légitimes :** dans ce cas, vous, ou un tiers, devez faire valoir un intérêt légitime qui n'entre pas en conflit avec les droits fondamentaux de l'individu.
- **Exécution d'un contrat :** ce fondement juridique permet le traitement des données s'il est nécessaire à l'exécution d'un contrat que vous avez signé, ou êtes en train de signer, avec l'individu.
- **Obligation légale :** les données peuvent être traitées si ce traitement vous est nécessaire pour vous conformer à vos obligations légales.
- **Intérêts vitaux :** le traitement peut également être effectué s'il est nécessaire pour protéger la vie d'une personne.
- **Mission de service public :** dans ce cas, le traitement des données doit être obligatoire pour effectuer une tâche légale dans l'intérêt public.

Notez que les gestionnaires de flotte pourront généralement avancer un **intérêt légitime** ou une **justification contractuelle** pour traiter les données personnelles.

Pour les gestionnaires de flotte, les **intérêts légitimes** peuvent couvrir des domaines tels que le traitement des données de kilométrage pour la gestion des contrats de location de véhicules, les données de carburant pour éviter les fraudes, ou l'utilisation des données sur le comportement de conduite pour aider à assurer la sécurité et à protéger la santé d'un conducteur.

Les motifs contractuels de traitement des données peuvent inclure l'utilisation des données télématiques afin d'enregistrer les heures de début et de fin de travail des conducteurs. Ces informations peuvent par exemple être couvertes par leur contrat de travail.

Il est également important de garder à l'esprit que tout individu a un « droit à l'oubli » et peut demander l'effacement de ses données. Cela peut avoir lieu si le consentement est annulé, si les données ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées, ou si l'individu s'oppose au traitement des données et qu'il n'existe aucun intérêt légitime justifiant de poursuivre ledit traitement.

OBJECTIFS DU TRAITEMENT DES DONNÉES

Dans le cadre du RGPD, l'objectif (ou les objectifs) du traitement des données doit être clairement défini à l'avance. L'objectif indiqué doit être spécifique et clairement défini, afin que la personne concernée puisse facilement le comprendre.

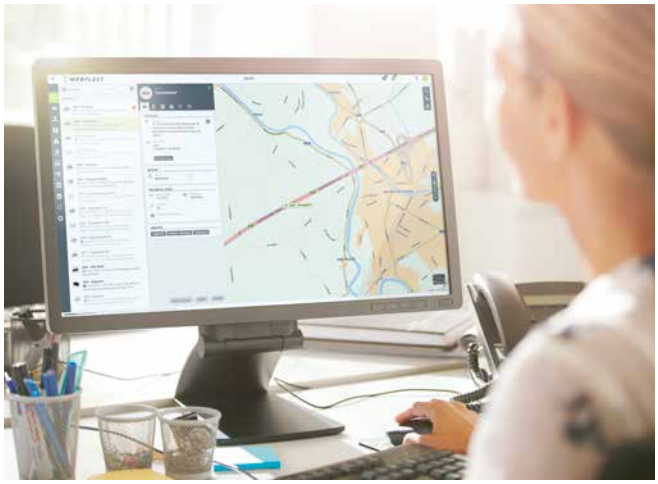
Les objectifs d'utilisation des données télématiques comprennent :

- La géolocalisation des véhicules en vue d'assurer la sécurité des ressources et d'optimiser l'efficacité de la flotte.
- La surveillance du comportement de conduite afin d'améliorer la sécurité des conducteurs et de diminuer les frais de carburant.
- La communication avec les conducteurs en vue d'améliorer la sécurité des employés et d'optimiser l'efficacité au travail.
- L'utilisation des données du tachygraphe et des heures de travail du conducteur pour assurer la conformité du temps de travail.
- Les rapports de gestion pour l'optimisation de l'activité, notamment via une amélioration du service client ou de l'efficacité de la flotte.
- L'intégration à un matériel ou une solution logicielle fourni par un tiers.

QUI DOIT ÊTRE RESPONSABLE ?

Il est important de souligner que chaque membre d'une entreprise doit se sentir responsable de la protection des données. En effet, les violations des données peuvent se produire en différents points de la chaîne logistique et de diverses manières.

Il est cependant conseillé de confier la responsabilité principale de la protection des données à une personne ou une équipe spécifique, afin de s'assurer que les processus visant à garantir la conformité de l'entreprise sont correctement gérés.



Il est peu probable que le service de la flotte soit responsable de la conformité, mais un gestionnaire de flotte peut jouer un rôle primordial de plusieurs autres manières, par exemple :

- en gérant les relations avec les fournisseurs et en s'assurant que des contrats sont signés ;
- en vérifiant qu'il existe un fondement juridique à l'utilisation des données relatives aux conducteurs ou aux membres du service de la flotte ;
- en obtenant l'accord des membres de l'équipe le cas échéant ;
- en communiquant avec le personnel et les principaux intervenants impliqués dans le service de la flotte afin de s'assurer qu'ils connaissent leurs responsabilités ;
- en fournissant les informations requises pour les pistes d'audit, par exemple les contrats et les formulaires de consentement.

À l'échelle de l'organisation, la responsabilité peut être confiée en majeure partie à un délégué à la protection des données (DPO). Néanmoins, les ressources humaines (RH), le département des opérations et le service informatique interviennent bien souvent dans ce processus.

COMMENT DÉVELOPPER **UN PLAN D'ACTION**

Dans le cadre du RGPD, un grand nombre de flux de données faisant partie de la chaîne logistique de la flotte peuvent être source de risque élevé pour les gestionnaires de flotte.

Par exemple, une entreprise peut collecter les données relatives au permis de conduire d'un conducteur auprès de l'autorité de délivrance et du conducteur lui-même, afin de déterminer s'il est autorisé à conduire. Ces données peuvent cependant ensuite être échangées avec les fournisseurs de services de prêt de véhicules, de gestion des risques ou d'assurance.

Étant donné le niveau de risque élevé, la première chose à faire pour une entreprise est de mener à bien une évaluation complète des risques, qui aidera à définir une image détaillée des différents points de la chaîne logistique où des données sont échangées et à identifier les sources potentielles de violation des données.

Des mesures peuvent alors être prises pour traiter chaque point et s'assurer que tout est mis en œuvre pour limiter et éliminer les risques pour la personne concernée, autant que faire se peut.

Dans les faits, le RGPD impose cette évaluation des risques, appelée **analyse d'impact relative à la protection des données (ou DPIA, pour Data Protection Impact Assessment)**, dans certaines situations.

Une DPIA est particulièrement utile lorsqu'un nouveau processus, un nouveau système ou une nouvelle technologie est déployé dans une entreprise. Mais elle peut également servir à démontrer les responsabilités dans le cadre du RGPD, permettant ainsi à une entreprise de se mettre en conformité et de prouver qu'elle a pris les mesures adéquates pour assurer sa conformité constante.

Le RGPD impose une DPIA lorsque le traitement des données « est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne physique ». Cela s'applique plus particulièrement aux situations dans lesquelles les données sont utilisées pour :

- une évaluation systématique et approfondie d'aspects personnels d'une personne physique, y compris le profilage ;
- le traitement de données sensibles à grande échelle ;
- la surveillance systématique de zones publiques à grande échelle.

Une majeure partie des données de flotte sont concernées par ces trois situations, par exemple l'utilisation des solutions télématiques pour surveiller les performances d'un conducteur, qui entre dans le cadre de la surveillance systématique des employés sur leur lieu de travail.

Les autorités européennes de protection des données ont émis des recommandations concernant les conditions requises pour réussir une DPIA, mais ses principes de base peuvent également être couverts par des meilleures pratiques en matière de protection des données personnelles.

Les actions suivantes permettent de faciliter la conformité légale :

- Mappage de tous les flux de données
- Analyse de la chaîne logistique
- Vérification de l'existence des contrats requis
- Établissement d'un processus pour les demandes de données
- Plan en cas de violation des données
- Vérification de la bonne compréhension de leur rôle par les employés

MAPPAGE DE TOUS LES FLUX DE DONNÉES

Le mappage de tous les flux de données qu'implique la chaîne logistique d'une flotte peut constituer un bon point de départ pour mener à bien une évaluation des risques adéquate.

Cela implique de répertorier tous les flux de données qui entrent ou sortent d'une entreprise, ainsi que les autres personnes ou organisations impliquées dans ces transactions.

Il peut être utile de représenter tous ces éléments sur un diagramme visuel qui permet une analyse rapide des liens entre les différents maillons de la chaîne.

Dans chaque situation, il convient d'identifier le contrôleur des données et le sous-traitant et de définir si les contrats adéquats sont en place.

Cela permettra à l'entreprise de savoir si elle est prête à l'entrée en vigueur du RGPD et où se trouvent les problèmes potentiels.

FLUX DE DONNÉES TRADITIONNELS DES FLOTTES

Les entreprises qui disposent d'une flotte de véhicules gèrent un grand nombre de flux de données, que ce soit en interne ou en externe. Voici quelques exemples d'organisations tierces avec lesquelles les données personnelles sont susceptibles d'être échangées :

- Fournisseurs de solutions télématiques et logicielles
- Entreprises de location longue durée
- Concessionnaires automobiles
- Compagnies d'assurance
- Fournisseurs de services de gestion des risques
- Fournisseurs de services de gestion des accidents
- Autorités de délivrance de plaques d'immatriculation
- Fournisseurs de services d'entretien, de maintenance et de réparation
- Fournisseurs de cartes de carburant

ANALYSE DE LA CHAÎNE LOGISTIQUE

Les entreprises peuvent être considérées responsables des violations dans l'ensemble de la chaîne logistique, ce qui signifie qu'il est primordial de s'assurer que tous les prestataires de services de la flotte qui traitent des données sensibles le font de manière sécurisée.

Chaque sous-traitant identifié lors du mappage des données doit pouvoir fournir des garanties suffisantes prouvant que les exigences du RGPD seront respectées et les droits des personnes concernées protégés.

Les mêmes conditions s'appliqueront à tous les nouveaux fournisseurs potentiels ; c'est pourquoi il est important de mettre en place une piste d'audit claire pour toutes les situations impliquant le traitement de données personnelles. Les gestionnaires de flotte doivent également garder à l'esprit que ces fournisseurs peuvent aussi eux-mêmes faire appel à des sous-traitants susceptibles d'utiliser les données.

> Les entreprises peuvent être tenues responsables des violations sur l'ensemble de la chaîne logistique

VÉRIFICATION DE L'EXISTENCE DES CONTRATS REQUIS

Dans le cadre d'un flux de données, il est important de définir si un nouveau consentement est requis pour s'assurer que la transaction est conforme au RGPD.

Par exemple, l'objectif visé par l'utilisation des données télématiques était-il clairement défini par le passé (réduction des frais de carburant, optimisation de la sécurité, etc.) ? Si ce n'était pas le cas, cela doit être modifié, afin que les employés sachent pourquoi leurs données personnelles sont requises.

Dès lors qu'un contrôleur de données fait appel à un sous-traitant, un contrat écrit stipulant les conditions d'utilisation doit être signé. Ces contrats aident également à s'assurer que les deux parties sont parfaitement informées de leurs responsabilités. Le RGPD répertorie les éléments que doit inclure un contrat entre le contrôleur et le sous-traitant.

ÉTABLISSEMENT D'UN PROCESSUS POUR LES DEMANDES DE DONNÉES

Conformément au RGPD, toute personne a le droit d'accéder à ses données personnelles détenues par une organisation. Dans le cas des données télématiques, il peut notamment s'agir des informations sur la position et les trajets, du kilométrage ou encore des statistiques relatives au comportement de conduite.

Si une personne demande à accéder à ses données, elle doit obtenir le détail des données conservées et une confirmation indiquant si elles font effectivement l'objet d'un traitement ou non. Ces informations doivent être fournies dans un délai d'un mois à compter de la réception de la demande. Ce délai peut être prolongé de deux mois supplémentaires si les demandes sont complexes ou nombreuses.

Afin de rester en conformité, les entreprises ont tout intérêt à établir un processus clair concernant le traitement de ces demandes. Celui-ci peut inclure l'affectation des responsabilités au personnel adéquat, ainsi que des mesures visant à vérifier l'identité de la personne qui effectue la demande.

Les entreprises doivent également s'assurer que les données sont facilement accessibles. Dans le cas des solutions télématiques, cela peut impliquer de s'associer à un fournisseur qui met à disposition des rapports complets et clairs qui précisent les données conservées sur chaque employé.

Les entreprises peuvent aussi créer une adresse e-mail spécifique à laquelle devront être envoyées les demandes. En appliquant des meilleures pratiques, chaque personne concernée pourrait accéder directement aux informations à distance, via un système sécurisé en libre-service.

> Si une personne demande à accéder à ses données, elle doit obtenir le détail des données conservées et une confirmation indiquant si elles font effectivement l'objet d'un traitement ou non

PLAN EN CAS DE VIOLATION DES DONNÉES

Bien qu'une grande variété de mesures puisse être prise pour réduire les risques, il est important de mettre en place un processus pour la gestion des violations des données.

Les violations des données incluent :

- l'accès aux données personnelles par un tiers non autorisé ;
- une violation délibérée ou involontaire par un contrôleur ou un sous-traitant ;
- l'envoi de données personnelles à un mauvais destinataire ;
- la perte ou le vol d'appareils informatiques contenant des données personnelles ;
- la modification des données personnelles sans autorisation ;
- la perte de disponibilité des données personnelles.

Des processus solides doivent être mis en place afin de détecter, analyser et signaler en interne les violations. Cela permet de s'assurer qu'une décision éclairée est prise quant à la gravité d'une violation et à l'intérêt de son signalement à l'autorité de surveillance concernée, ce dernier devant avoir lieu dans un délai de 72 heures si possible. Lorsqu'il existe un fort risque que la violation affecte les droits et libertés d'un individu, cet individu doit également en être informé.

Pour faciliter ce processus, les employés peuvent être formés à détecter les violations et à les signaler à la personne adéquate dans leur entreprise.

LISTE DE VÉRIFICATION EN CAS DE VIOLATION DES DONNÉES

Afin de réagir de manière adéquate en cas de violation des données, les entreprises doivent s'assurer qu'elles :

- disposent d'un processus permettant d'évaluer le risque potentiel pour les personnes concernées en cas de violation ;
- sont capables d'identifier l'autorité de surveillance adéquate pour les activités de traitement ;
- disposent d'un processus afin de signaler toute violation à l'autorité de surveillance adéquate dans les 72 heures suivant sa détection, même si toutes les informations ne sont pas encore disponibles ;
- connaissent quelles sont les informations à fournir à l'autorité de surveillance concernée en cas de violation ;
- disposent d'un processus visant à informer les personnes concernées par la violation lorsque celle-ci risque de menacer leurs droits et leurs libertés ;
- informent immédiatement les personnes concernées ;
- connaissent quelles sont les informations à fournir aux personnes concernées par une violation, et sont en mesure de les aider à se protéger de ses conséquences ;
- documentent toutes les violations, même celles qui ne doivent pas nécessairement être signalées[1].

[1] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

VÉRIFICATION DE LA BONNE COMPRÉHENSION DE LEUR RÔLE PAR LES EMPLOYÉS

On croit parfois à tort que la protection des données relève uniquement de la responsabilité du contrôleur de données désigné dans l'organisation. Cependant, l'ensemble du personnel peut jouer un rôle en vue de s'assurer que l'entreprise demeure conforme aux exigences légales. Même les tâches du quotidien telles que l'envoi d'un e-mail peuvent être à l'origine d'une violation des données si des données personnelles sont accidentellement envoyées à une personne qui n'est pas autorisée à les consulter.

C'est pourquoi il est important de créer une véritable culture d'entreprise et d'aider tous les employés à s'impliquer dans la protection des données personnelles.

Pour y parvenir, la communication est primordiale : des mesures simples telles que des bulletins d'information envoyés par e-mail au personnel ou encore des formations et des ateliers ciblés peuvent vous aider. Il est également conseillé aux entreprises de s'assurer que leur personnel connaît ses responsabilités en matière de protection des données, notamment toutes les activités susceptibles de provoquer une violation des données, et qu'il sait comment réagir en cas de suspicion de violation des données.

Dans le cadre de la gestion de flotte, la communication peut devenir un véritable défi : le personnel passant beaucoup de temps sur la route, il peut être recommandé de réfléchir au mode de communication. Vous pouvez par exemple envoyer les messages aux employés sur leur terminal embarqué ou créer un guide qui sera placé dans chaque véhicule. Toutes ces actions peuvent faire partie d'une approche structurée et méthodique de la protection des données. En adoptant des meilleures pratiques, les entreprises peuvent être en position d'assurer leur mise en conformité légale.

Cela peut nécessiter un effort considérable, mais il est indispensable d'y consacrer du temps et des ressources, afin de s'assurer que les systèmes adéquats sont en place et surveillés en continu.

Il est également vital de faire appel à des fournisseurs capables de respecter ces normes drastiques en matière de protection des données. Cela signifie qu'il faut passer en revue les relations entretenues avec les fournisseurs existants afin de vérifier qu'en cas de partage de données, l'utilisation de ces dernières a été explicitement acceptée. Les meilleures pratiques peuvent notamment inclure le recours à des accords écrits spécifiant les conditions d'utilisation.

> Il est important de créer une véritable culture d'entreprise et d'aider tous les employés à s'impliquer dans la protection des données personnelles

EN QUOI TOMTOM TELEMATICS **PEUT VOUS AIDER À RESPECTER LES OBLIGATIONS DU RGPD**

Pour les gestionnaires de flotte, le RGPD peut s'apparenter à un véritable labyrinthe réglementaire.

Bien que les nouvelles règles doivent être mises en perspective (comme un moyen d'étendre et de renforcer les lois existantes sur la confidentialité et la sécurité des données), le poids des responsabilités a sans nul doute augmenté.

La non-conformité n'est plus une option. La relation entre les gestionnaires de flotte et leurs conducteurs n'est pas la seule à être désormais mise en avant : celle liant les gestionnaires (contrôleurs) et les sous-traitants, notamment les fournisseurs de solutions télématiques, l'est tout autant.

Les entreprises doivent pouvoir être certaines que leur système télématique respecte les nouvelles règles, afin de ne pas risquer de pénalités dues à des violations de la sécurité et de la confidentialité des données.

Chez TomTom Telematics, nous travaillons sur les exigences du RGPD depuis 2012, lors de la publication des premières ébauches. C'est pourquoi cette réglementation a joué un rôle considérable dans la conception des solutions que nous fournissons à nos clients, afin qu'ils soient assurés que nous avons pris toutes les mesures nécessaires pour que vous soyez entre de bonnes mains.

> TomTom Telematics travaille sur les exigences du RGPD depuis 2012

LA CLÉ ?
LA SÉCURITÉ DE L'INFORMATION

Le principe de protection des données dès la conception et par défaut, qui fait partie intégrante du RGPD, renforce encore l'importance de la sécurité des données.

Dès le départ, il est obligatoire de prendre des mesures techniques et organisationnelles visant à démontrer que vous avez intégré la protection des données aux activités de traitement des données.

Cela oblige donc les personnes en charge de la conception des technologies à prendre en compte la confidentialité. TomTom Telematics, qui agit en tant que sous-traitant pour les données personnelles de ses clients, s'est engagé à respecter cette obligation dès la publication des premières ébauches du RGPD, en 2011. Nous expliquons ci-dessous en quoi nos solutions, contrôlées et auditées par notre délégué à la protection des données (DPO), s'y conforment.

SÉCURITÉ DES DONNÉES CERTIFIÉE

Nous avons mis en place des règles très strictes en matière de sécurité et de confidentialité des données et avons défini des meilleures pratiques afin d'assurer le respect des normes les plus drastiques. Cela est confirmé par la certification ISO/IEC 27001:2013 qui a été accordée à TomTom Telematics et à laquelle tous les employés sont tenus de se conformer.

Notre système de gestion de la sécurité de l'information (ISMS) couvre tous les processus métier critiques indispensables à la sécurisation des informations liées à la plateforme de services TomTom Telematics. Conformément à la norme ISO/IEC 27001:2013, cela inclut l'architecture, l'ingénierie, l'assurance qualité et les services informatiques, ainsi que nos data centers sécurisés situés au sein de l'Union Européenne. **La connexion chiffrée sécurisée et le transfert des données vers notre plateforme de services répondent aux normes les plus strictes des certificats SLL EV (Extended Validation).**

Nos processus et principes de codage sécurisés assurent un cycle de vie du produit flexible. Ils incluent notamment une conception et un codage vérifiés par les pairs ; des guides de style ; un test de charge / fonctionnel pour l'assurance qualité ; la gestion des versions et des modifications ; un examen du code statique.

Nous suivons également les programmes suivants : formation à la sécurité pour nos employés ; test et vérification de la sécurité lors de l'implémentation ; renforcement des systèmes ; gestion de la vulnérabilité / des correctifs ; test de la sécurité des applications Web.

Un examen régulier des obligations légales ou sécuritaires pouvant avoir un impact sur notre plateforme de services télématiques ou nos actifs informationnels est réalisé par l'équipe en charge de notre système de gestion de la sécurité de l'information (ISMS).

Notre système de gestion de la sécurité de l'information comprend :

- **des politiques détaillées relatives à la sécurité**, qui donnent des pistes de gestion et soutiennent le système de gestion de l'information et toutes les activités opérationnelles ;
- **des protocoles de sécurité pour les ressources humaines**, incluant le choix des bons employés et une formation personnalisée en continu ;
- **des contrôles de gestion des actifs**, notamment l'inventaire, la propriété et la maintenance tout au long de leur cycle de vie, afin d'assurer l'identification précise, le bon étiquetage et l'affectation aux bonnes personnes des actifs ; ces démarches incluent notamment la gestion de la propriété intellectuelle de l'entreprise et des données client.
- **des contrôles d'accès** limitant l'accès aux données en fonction des besoins de l'utilisateur ; des contrôles supplémentaires permettent d'éviter tout accès non autorisé ;
- **des technologies de cryptage**, qui assurent la confidentialité et l'intégrité des données de nos clients et de nos systèmes opérationnels.
- **un système assurant la sécurité physique et environnementale**, qui inclut des data centers de niveau 3+, une configuration active visant à assurer la récupération après sinistre et une disponibilité élevée, régulièrement testées ;
- **un système assurant la sécurité opérationnelle**, s'appuyant sur des bases en matière de sécurité et des processus gérés, stricts et reproductibles ;
- **un système assurant la sécurité des communications** par le biais de mesures comme la ségrégation de réseau, la séparation VLAN, un DMZ avec pare-feu multi-niveaux, un contrôleur d'accès au réseau (NAC) et un cryptage par défaut suivant les dernières normes du secteur.

LES DONNÉES DE VOS CONDUCTEURS : VOUS AVEZ LE POUVOIR

Dans la mesure où les données télématiques sont liées à vos conducteurs, vous êtes le seul à décider comment et pourquoi elles sont utilisées.

Dans le cadre de notre engagement en faveur de la confidentialité des données des conducteurs, nous travaillons en partenariat avec des groupes et des comités de travail spécialisés dans la protection des données. Afin de s'assurer que chacun sait comment ses données sont utilisées, nous fournissons du matériel explicatif, notamment des manuels en ligne et des supports de formation. Ceux-ci sont accessibles via les informations de support "Découvrir WEBFLEET" et les guides d'utilisation sont disponibles sur notre portail client TomTom Telematics.

En outre, la solution TomTom Telematics est hautement personnalisable, ce qui vous permet de définir les données recueillies, ainsi que quand et pendant combien de temps elles sont conservées.

STOCKAGE ET RÉTENTION DES DONNÉES

Le RGPD impose que vous répertoriiez toutes les données personnelles que vous conservez, ainsi que leur origine et avec qui vous les partagez.

La plateforme de services TomTom Telematics propose des options par défaut pour le stockage des données en se basant sur les besoins classiques des clients, mais vous pouvez ensuite les personnaliser.

Les messages texte, les messages liés aux commandes et au statut des véhicules, les données de position et les données liées aux événements de conduite et aux vitesses excessives sont stockés pendant 60 jours. Les données de trajet sont enregistrées pendant deux années civiles complètes en plus de l'année civile en cours. Les rapports archivés sont quant à eux conservés pendant 36 mois.

Toutes les données client traitées par TomTom Telematics sont conservées dans des data centers situés dans des bunkers pauvres en oxygène offrant une double redondance.

CONFIDENTIALITÉ ET ACCÈS AUX DONNÉES

Le RGPD impose que TomTom Telematics fasse l'objet de contrôles et d'audits visant à assurer sa conformité en matière de confidentialité des données.

WEBFLEET est uniquement accessible avec un accès sécurisé nécessitant un identifiant personnel et un mot de passe. Conformément au RGPD, l'accès à l'ensemble des données WEBFLEET par tous les utilisateurs est rarement nécessaire ou approprié.

Les données mises à disposition des utilisateurs enregistrés peuvent donc être restreintes selon les besoins spécifiques de chacun. Les responsables des ressources humaines, les directeurs financiers et les professionnels des ventes ou des opérations, par exemple, n'auront pas besoin d'accéder aux mêmes données dans le cadre de leurs fonctions.

Les conducteurs de véhicules équipés de notre solution de gestion de flotte pourront opter pour le mode Trajet professionnel ou Trajet privé, afin d'activer ou de désactiver le suivi de la position de leur véhicule.

TomTom Telematics aide également ses clients à respecter les droits individuels en matière d'accès aux données et de suppression des données.

Lorsque des données sont effacées, elles sont marquées comme déréférencées puis écrasées de façon à empêcher leur utilisation par d'autres parties.

TomTom Telematics fait l'objet de contrôles et d'audits visant à assurer sa conformité en matière de confidentialité des données

DIX QUESTIONS À POSER À VOTRE FOURNISSEUR DE SERVICES TÉLÉMATIQUES

Nous avons expliqué en quoi TomTom Telematics vous permet de remplir vos obligations, en vous assurant que votre fournisseur favori vous aide à respecter la législation.

1. Agissez-vous en tant que sous-traitant ou contrôleur de données selon les définitions du RGPD ?
2. Votre système respecte-t-il les exigences du RGPD et les normes internationales en matière de sécurité et de confidentialité des données ?
3. Quels types de données conservez-vous ?
4. Où et pendant combien de temps les données personnelles de vos conducteurs sont-elles conservées ?
5. Les clients peuvent-ils décider de la durée de rétention de leurs données ?
6. Votre système permet-il la gestion des utilisateurs en restreignant l'accès aux données aux seules personnes qui en ont besoin ?
7. Votre système permet-il la suppression des données personnelles ?
8. Les données des clients sont-elles mises à disposition des tiers ?
9. Les conducteurs ont-ils la possibilité de protéger leurs données lorsqu'ils effectuent des trajets privés ?
10. Fournissez-vous à vos clients des supports de communication à partager avec les conducteurs, leur expliquant comment leurs données personnelles sont utilisées ?

TOMTOM TELEMATICS

CLAUSE DE NON-RESPONSABILITÉ : les informations figurant dans la documentation TomTom Telematics et en ligne sont fournies à titre informatif uniquement et expriment notre opinion sur le sujet abordé. Elles ne sauraient constituer un conseil juridique sur le sujet. En outre, les informations contenues dans ces documents et en ligne pourraient ne pas refléter l'évolution des exigences juridiques. Vous ne devez pas agir en vous appuyant sur ces informations sans obtenir au préalable un avis juridique.