MICHELIN

UNE MEILLEURE FAÇON D'AVANCER

LES FONDAMENTAUX

POLITIQUE GLOBALE DE PROTECTION

DES DONNÉES À CARACTÈRE PERSONNEL

ÉDITO

Michelin a pour ambition de s'imposer comme leader mondial en mobilité durable et en innovation tout en contribuant à répondre aux enjeux de société et en pratiquant des valeurs de respect des personnes essentielles à ses yeux.

Michelin accorde ainsi une grande importance à la protection des données et informations personnelles et souhaite, dans un souci de transparence et de clarté, par l'intermédiaire de la présente politique, vous informer de la manière dont elle collecte et traite les données de ses employés, clients ou fournisseur dans le monde entier.

Cette politique vient consolider son code d'Éthique et constitue un vecteur de confiance pour les personnes. La protection des données et informations personnelles n'est pas l'affaire des seuls spécialistes mais aussi celle de tout un chacun au quotidien.

Merci pour votre engagement à assurer la protection des données et informations personnelles dans le respect des principes et lignes directrices énoncés dans cette politique.

Le Comité de Protection des Données Personnelles

OBJECTIF

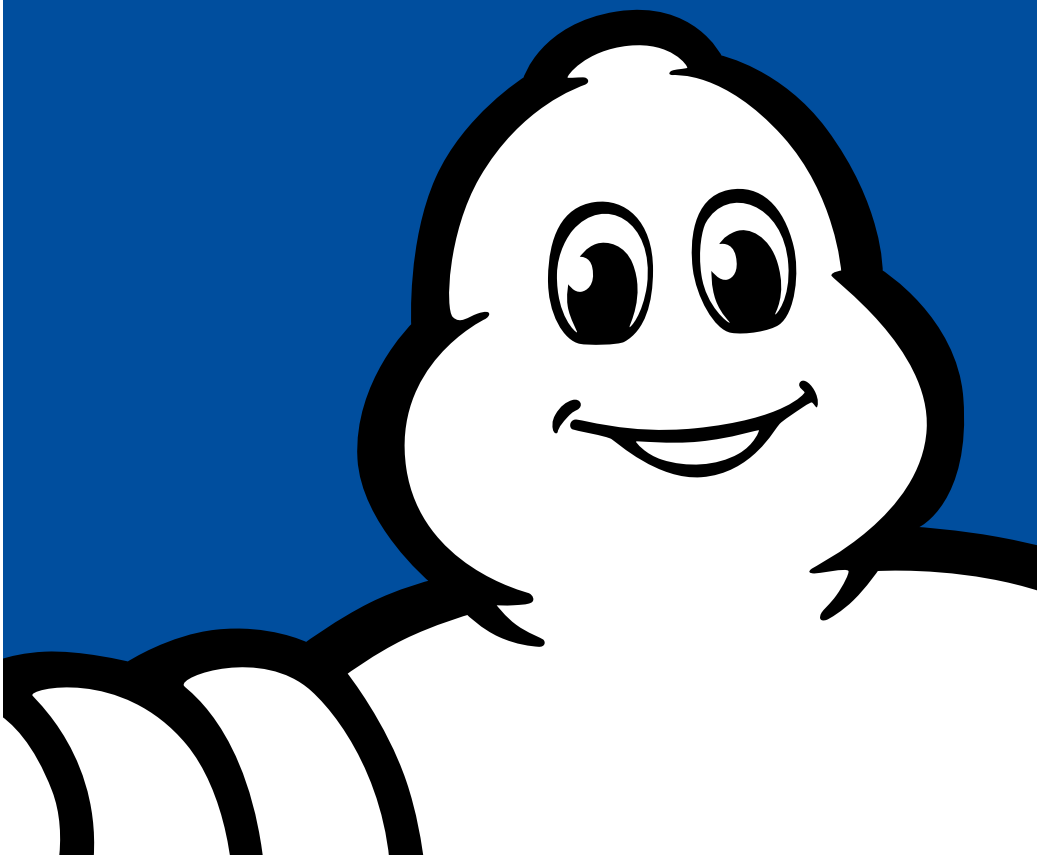
Cette politique globale de protection des données à caractère personnel s'appuie sur la Directive Groupe sur les données personnelles et sur les Règles d'Entreprise Contraignantes de Michelin qui s'imposent à toutes les sociétés du Groupe qui y ont adhéré, qu'elles soient situées dans ou hors du territoire de l'Union européenne.

PÉRIMÈTRE

Cette politique vise à décrire les règles de bonne conduite dont le respect est attendu des collaborateurs de Michelin dans le monde entier et est applicable depuis le 7 juin 2017.

SOMMAIRE

INTRODUCTION



Michelin est engagé dans une politique d'innovation et de transformation numérique fondée sur le respect de valeurs éthiques et d'une culture d'entreprise fortes. La confiance, l'intégrité et la protection des données à caractère personnel et de la vie privée sont au cœur des préoccupations de Michelin et représentent un défi et un enjeu importants. La protection de ces données constitue en effet, un atout compétitif majeur et un vecteur de confiance dans les relations avec les partenaires commerciaux, les clients et les employés.
La présente politique vise à décrire les règles de bonne conduite dont le respect est attendu des collaborateurs de Michelin dans le monde entier pour assurer la protection des données à caractère personnel et ainsi la protection de la vie privée des individus, et notamment des employés, clients et partenaires commerciaux de Michelin.

La présente politique s'appuie sur les Règles d'Entreprise Contraignantes de Michelin (Binding Corporate Rules) qui ont été validées par la Commission Nationale de l'Informatique et des Libertés (CNIL) en France ainsi que par l'ensemble des autorités de protection des données en Europe. Ces règles doivent être respectées à l'occasion des traitements de données à caractère personnel (tels que définis ci-dessous) qui sont mis en œuvre dans cette zone lorsque lesdites données sont ensuite transférées hors de l'Union européenne et à l'intérieur du Groupe pour faire l'objet d'un autre traitement. Les Règles d'Entreprise Contraignantes s'imposent à toutes les sociétés du groupe qui y ont adhéré, qu'elles soient situées dans ou hors du territoire de l'Union européenne.

La présente politique indique également le comportement responsable et éthique que chaque collaborateur doit observer à l'occasion de la collecte et du traitement de données à caractère personnel.

Elle complète les lois locales existantes mais ne les remplace pas. En cas de conflit entre cette politique et la loi nationale applicable ou lorsque la loi nationale a des exigences plus strictes, la loi nationale prévaut.

Elle pourra être amenée à évoluer en fonction du contexte légal et réglementaire applicable.

1. CONCEPTS

Pour bien comprendre la réglementation sur la protection des données à caractère personnel, il est important d'en maîtriser les concepts.

1.1. Données à caractère personnel

Il s'agit de toute information relative à une personne physique permettant son identification directe ou indirecte, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Sont donc des données à caractère personnel des données qui, seules ou combinées entre elles, peuvent être rattachées à une personne physique.

Exemple : l'identifiant Michelin, le nom, le numéro de sécurité sociale, l'adresse, la fonction, les hobbies, les données de localisation d'un individu.

1.2. Données à caractère personnel sensibles

Il s'agit des données à caractère personnel faisant apparaître de façon directe ou indirecte les origines raciales, ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale des personnes, les condamnations pénales ou infractions ou qui sont relatives à leur santé ou à leur vie sexuelle.

1.3. Personne concernée

La personne concernée désigne la personne à laquelle se rapportent les données qui font l'objet d'un traitement.

Exemple : le candidat dont on étudie la candidature, le client dont on traite la réclamation, le salarié dont on gère les congés...

1.4. Responsable d'un traitement de données à caractère personnel

Il s'agit de la personne physique ou morale, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens d'un traitement de données à caractère personnel.

Exemple : l'établissement qui met en place un dispositif de vidéosurveillance, l'entreprise qui introduit un nouveau système de gestion des déplacements professionnels pour ses employés.

1.5. Sous-traitant

De façon générale, toute société qui traite des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant.

Exemple : un prestataire d'hébergement de données ou une société gérant un centre d'appels.

1.6. Traitement de données à caractère personnel

Constitue un traitement de données à caractère personnel (ci-après « Traitement ») toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toutes autres formes de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel.

2. PRINCIPES DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

La réglementation relative à la protection des données à caractère personnel se décline en plusieurs grands principes qu'il vous est demandé d'observer scrupuleusement. Ne pas les respecter, c'est prendre et faire prendre le risque à Michelin d'être lourdement sanctionné.

2.1. Légalité

Chaque collaborateur s'interdit de mettre en œuvre un Traitement à partir de données collectées de manière illicite c'est-à-dire à l'insu des personnes et/ou pour une finalité de traitement qui serait illégale.

Avant de mettre en œuvre un Traitement, il faut vérifier que l'objectif du traitement qui sera mis en œuvre est en conformité avec la réglementation applicable à notre secteur d'activité.

Il faut également vérifier auprès du département DGD/Data Privacy et/ou du Privacy Officer de votre pays que le Traitement que vous envisagez de mettre en œuvre est conforme à la réglementation locale applicable.

2.2. Loyauté et transparence

Il faut être transparent vis-à-vis des personnes concernées : les données à caractère personnel ne doivent pas être collectées (sans le consentement des personnes concernées lorsqu'il est requis) et traitées à l'insu des personnes concernées.

Avant de mettre en œuvre un Traitement, vérifiez que les personnes concernées ont été informées :

- des traitements portant sur les données à caractère personnel les concernant ;
- de leurs droits (droits d'accès, de rectification…).

Pour cela, il faut préparer une mention permettant de diffuser clairement cette information (sur un site internet, par affichage d'un panneau, dans un contrat…).

Ne vous procurez pas de données à caractère personnel auprès de tiers sans vous être assuré au préalable que ces tiers ont les droits nécessaires pour collecter et transmettre de telles données.

2.3. Finalité et légitimité

Définissez clairement les objectifs de votre Traitement : les données doivent uniquement être collectées pour des finalités déterminées, explicites, légitimes et compatibles avec les finalités initiales.

Interdisez-vous toute réutilisation des données pour des finalités incompatibles avec les finalités initiales.

Exemples : envoi d'une newsletter à un candidat à un emploi en l'absence de demande expresse de sa part, envoi de prospection par mél à des clients ayant participé à un jeu concours en l'absence de recueil de leur consentement express, utilisation des images prises par une caméra de vidéosurveillance pour compter le temps de travail effectif d'un salarié.

2.4. Nécessité et proportionnalité

Ne soyez pas excessif dans la collecte de vos données : gardez en tête que seules peuvent être collectées les données à caractère personnel strictement nécessaires à la réalisation du Traitement.

En particulier, il est interdit de collecter et de traiter des données à caractère personnel sensibles si ces données ne sont pas strictement indispensables à la finalité de votre Traitement. Vérifiez auprès du département DGD/Data Privacy ou du Privacy Officer de votre pays que vous êtes autorisés à collecter ces données au titre de la réglementation applicable dans votre pays/zone.

Dès la création de votre Traitement, définissez la durée pendant laquelle vous aurez besoin de conserver les données pour pouvoir atteindre l'objectif du Traitement. Mettez en place les procédures de purge des données.

2.5. Qualité

Tenez à jour vos bases de données : régulièrement, assurez-vous que les données à caractère personnel que vous êtes amené à traiter dans le cadre de votre activité sont exactes et ne sont pas périmées et si besoin, mettez à jour ces données.

Assurez-vous qu'aucune donnée excessive et non objective ne figure dans les zones de commentaires libres.

2.6. Respect des droits des personnes

Donnez aux personnes concernées les moyens d'exercer leurs droits.

Les personnes dont vous traitez les données ont le droit d'accéder aux données qui les concernent et d'en demander la rectification ou la suppression dans certains cas. Elles peuvent également demander à ne plus recevoir de prospection commerciale.

Respectez les droits des personnes concernées et aidez l'entreprise à répondre dans les meilleurs délais aux demandes qui lui sont adressées en faisant remonter toute demande à votre référent protection des données, s'il en existe dans votre pays/zone et/ou au Privacy Officer de votre pays/zone au sein de DGD.

2.7. Sécurité et confidentialité

Protégez vos fichiers et sécurisez les données : prenez soin de respecter les mesures de sécurité définies par le Groupe notamment dans les documents diffusés au niveau local tels que la charte des systèmes d'information.

Les données à caractère personnel que vous traitez doivent rester confidentielles : prenez soin de ne pas divulguer ces informations auprès d'autres services ou auprès de tiers qui ne seraient pas habilités à en prendre connaissance. Les données doivent faire l'objet d'un stockage et de transferts sécurisés – par exemple via l'utilisation de la solution Securitybox.

Si vous avez besoin de sous-traiter une partie ou la totalité de la mise en œuvre d'un Traitement, vous devez imposer contractuellement au sous-traitant des obligations fortes de sécurité et de confidentialité des données. Pour cela, il vous faut impérativement vous rapprocher du service achat local en coordination avec un responsable de la sécurité de l'information et le Privacy Officer de votre pays/zone afin que les clauses appropriées soient intégrées dans le contrat avec le dit sous-traitant.

Enfin, nous sommes tous acteurs et responsables quant à la bonne protection des données personnelles. En cas de détection d'une situation anormale, d'une fuite de données personnelles, d'une publication anormale de données, il convient d'alerter le plus rapidement possible les équipes en charge de la protection des informations de Michelin.

2.8. Encadrement des transferts de données à caractère personnel en provenance de l'Union européenne à destination hors Union européenne

Maîtrisez les flux de données à caractère personnel : ne transférez des données à caractère personnel vers un autre pays qu'après avoir vérifié auprès de votre Privacy Officer si et dans quelles conditions vous êtes autorisé à le faire.

3. EN PRATIQUE

	À FAIRE	À NE PAS FAIRE
Lors de la collecte de données	Identifier précisément les finalités initiales de la collecte des données pour les rendre déterminées et explicites. Examiner les formalités réalisées pour le Traitement et la nature des informations collectées pour déterminer si les finalités de la collecte et du Traitement des données sont déterminées et explicites.	Collecter des données dont le responsable de traitement ne connaît pas l'origine. Traiter des données interdites (santé, religion, opinions politiques, notamment) sauf si la loi nationale l'autorise ou dans le cas des exceptions prévues par la loi. Collecter des données sans informer les personnes sur les finalités de la collecte et du traitement des données. Utiliser un Traitement pour d'autres finalités sans se poser la question de la compatibilité de ces nouvelles finalités avec les finalités initiales. Collecter plus de données que celles nécessaires au traitement.
Qualité des données	Mettre à jour périodiquement les traitements et fichiers de données à caractère personnel. Pour les zones de commentaires libres, s'assurer que seules des données nécessaires au Traitement sont collectées.	Dans les zones de commentaires libres : - appréciations d'ordre personnel, jugements de valeur : expressions injurieuses, désobligeantes, blessantes ; - appréciations sur le comportement de la personne (exemples : « personne timide », « mauvais caractère », etc.) ; - données sur l'origine raciale, ethnique, opinions politiques, religieuses, philosophiques, appartenance syndicale, santé, vie sexuelle.
Durée de conservation des données	Vérifier qu'il existe des durées de conservation pour chaque catégorie de données traitées au sein du Traitement. Apprécier la durée de conservation par rapport à la finalité poursuivie. Mettre en place des procédures de purge appropriées.	Procéder à des extractions Excel des données d'une application et conserver ce fichier sans s'assurer de respecter la durée de conservation initiale. Encourager ou faciliter les extractions Excel. Ne pas définir de durée de conservation dans les applications lors de la phase de développement.
Destinataires des traitements	Identifier les destinataires de chaque Traitement en se référant notamment à la formalité préalable effectuée.	Communiquer les données à des tiers sans vérifier leur habilitation.

	À FAIRE	À NE PAS FAIRE
Transferts de données	Identifier les transferts réalisés hors de l'Union européenne. Identifier si les transferts ont lieu à l'intérieur du Groupe ou non. Vérifier à quel cadre juridique est soumis le transfert vers les pays identifiés.	Mettre en œuvre des transferts de données vers des pays hors Union européenne n'ayant pas de protection adéquate sans encadrement juridique.
Sécurité	Mettre en œuvre des mesures techniques et organisationnelles appropriées pour protéger la sécurité et la confidentialité des données à caractère personnel pour le traitement effectué par le responsable du traitement et/ou par le sous-traitant.	Mettre en œuvre et maintenir des mesures inappropriées pour protéger la sécurité et la confidentialité des données à caractère personnel.
Information des personnes concernées	S'assurer que les personnes concernées ont bien été informées du Traitement qui va être mis en œuvre. Le cas échéant, informer les personnes concernées au moyen d'une mention.	Ne pas apposer de mention relative à la collecte et au traitement des données personnelles ou la faire figurer de telle manière qu'elle soit peu visible.
Respect du droit des personnes	En cas de réception d'une demande d'exercice d'un droit d'accès, de rectification ou d'opposition, se référer à la procédure de gestion des droits en vous adressant à votre référent local protection des données.	Ne pas respecter le délai légal pour envoyer une réponse. S'abstenir de répondre ou de traiter les demandes légitimes d'opposition, d'accès ou de rectification. Imputer des frais à la personne exerçant son droit d'opposition ou des frais supérieurs au coût de la copie en cas de demande de copie. Considérer comme abusive toute demande d'accès d'une personne sur les informations la concernant.
Fuite de données	En cas de suspicion de fuite de données, prévenir le correspondant sécurité.	Tenter de régler le problème localement sans en informer le DPO – ignorer le problème.

4. POUR ALLER PLUS LOIN

4.1. Personnes à contacter

En cas de difficulté dans la compréhension ou l'application des règles définies dans la présente politique, vous pouvez contacter votre référent local protection des données.

Michelin
Direction Groupe Marques et Relations extérieures
23 place des Carmes-Déchaux
63040 Clermont-Ferrand Cedex 9 - France

www.michelin.com

Conception et réalisation : $\overline{w}$

Référence du document : Politique globale de protection des données à caractère personnel
Auteur du document : DGD
Niveau de confidentialité : D3
Date de mise à jour : juin 2017
Conservation : WA+10

Référence : REF_020_DGD (FR)


MICHELIN
UNE MEILLEURE FAÇON D'AVANCER