UFMD
Union française du marketing direct & digital

PROTECTION DONNÉES

RÉGLEMENTATION GÉNÉRALE

AACC

ARPP
autorité de
régulation professionnelle
de la publicité

Cercle Marketing Direct
à l'heure du digital

FEDMA

MMA
MOBILE MARKETING ASSOCIATION

LA POSTE
SOLUTIONSBUSINESS

fevad
www.fevad.com

SRI
LES RÉGIES INTERNET

UDECAM

www.fevad.com

Règlement Général sur la protection des données

INFO ou INTOX ?

Affirmation n°1: Le Règlement concerne uniquement les grandes entreprises

Faux

Le Règlement s'applique à tout traitement de données à caractère personnel, qu'elles soient traitées par de grandes ou petites entreprises. Par conséquent, il concerne toutes les entreprises, petites et grandes. Le Règlement comprend certains aménagements pour les PME afin de leur éviter une surcharge administrative. Il est en par exemple ainsi en matière de registre de leurs activités de traitement, dont l'obligation de tenue est levée à moins que celle-ci soit susceptible de comporter un risque pour les droits et libertés des personnes concernées.

Affirmation n° 2: Le Règlement s'applique également à des entreprises basées en dehors de l'Europe

Vrai

Le Règlement concerne toutes les entreprises basées dans les 28 Etats membres de l'Union Européenne même si le traitement des données a lieu en dehors de l'Union européenne. En outre, le Règlement concerne également les entreprises non basées dans l'Union européenne, si le traitement des données de personnes qui se trouvent sur le territoire de l'Union européenne, est lié à une offre de biens et services (y compris des biens et services gratuits) dans l'Union européenne, ou si ces entreprises contrôlent le comportement des personnes dans l'Union européenne par le biais de l'utilisation de cookies ou toute autre technologie similaire.

Affirmation n°3: Le Règlement ne concerne que les données en ligne

Faux

Le Règlement est technologiquement neutre.
Aussi, les nouvelles règles s'appliquent à toutes les données personnelles, en ligne et hors ligne.

Affirmation n° 4: Je ne traite que des données en B2B, le Règlement ne me concerne pas

Faux

Le Règlement s'applique au traitement de données personnelles, et ne fait pas de distinction entre les données personnelles en B2B et B2C.
Les données personnelles dans le secteur du B2B sont celles qui identifient une personne physique telles que les adresses e-mail de travail, les lignes de téléphone directes, le nom et intitulé du poste

ainsi que l'adresse postale du lieu de travail

Affirmation n° 5: le Règlement s'applique quel que soit le mode de traitement des données

Vrai

Le Règlement s'applique aux données personnelles traitées entièrement automatiquement (par exemple, le profilage), partiellement automatiquement, ou par tout autre moyen, y compris des processus manuels (à savoir par un être humain).

Affirmation n° 6: Je dois simplement revoir mes politiques et clauses de confidentialité pour me conformer au Règlement

Faux

Le Règlement augmente le niveau des obligations déjà existantes en matière de protection des données, par exemple, le consentement doit être donné sans ambiguïté et les entreprises devront fournir aux personnes plus d'informations au sujet de leurs activités de traitement de données à caractère personnel.

Le nouveau Règlement comprend également de nouvelles obligations.

Il en est ainsi de la notification des violations de la sécurité des données, de la mise en place du principe de protection des données dès la conception (principe de Privacy by design) et faire en sorte que les paramètres de confidentialité soient initialement configurés de manière à protéger les données des personnes (principe de Privacy by défault).

Le Règlement comporte aussi de nouveaux droits pour les particuliers, tel que le droit à la portabilité des données.

Revoir les politiques et clauses de confidentialité pour assurer leur conformité avec les nouvelles exigences en matière d'information que les entreprises doivent fournir aux personnes, n'est qu'une action parmi tant d'autres nécessaires à la mise en œuvre des nouvelles règles.

De nouvelles procédures doivent être mises en place.

En outre, le principe de responsabilité (accountability) mis en place dans le Règlement encourage les entreprises à adopter une nouvelle approche proactive de la protection de la vie privée dans leur gestion quotidienne de données, afin d'être en mesure de démontrer aux autorités nationales de protection des données qu'elles sont conformes au Règlement.

Affirmation n° 7: J'ai le consentement des personnes pour l'utilisation de leurs données personnelles, je n'ai donc pas besoin d'appliquer le Règlement

Faux

Le Règlement augmente les normes de protection des données déjà existantes, notamment en matière de consentement.

Le consentement doit être donné sans ambiguïté, et ne peut pas être déduit de l'inaction, mais doit être le résultat d'une action positive de la personne. Par conséquent, la façon de recueillir le consentement des personnes devra être revue. Cependant, le Règlement reconnaît d'autres

fondements légaux alternatifs pour le traitement des données personnelles.

Affirmation n° 8: En affichant le bandeau des cookies sur mon site, je suis déjà conforme au Règlement

Faux

Il est utile de rappeler que le Règlement technologiquement neutre s'appliquera au traitement des données personnelles au sens large, et pas seulement dans un environnement en ligne.
La question de l'information sur l'utilisation des cookies et de l'obtention de l'accord des utilisateurs, par le biais d'un bandeau par exemple, découle de la Directive vie privée et communications électroniques.
Le Règlement est plus large et inclut de nouvelles exigences en matière d'information des personnes comme le recueil de leur consentement, qui auront des conséquences en matière de cookies.
La Directive vie privée et communications électroniques est en cours de révision afin d'assurer sa cohérence avec le Règlement.

Affirmation n° 9 : le Règlement impose à toutes les entreprises de notifier leurs failles de sécurité

Vrai

Alors que la Règlementation en vigueur n'impose qu'aux opérateurs télécoms de procéder à des notifications de leurs failles de sécurité, le nouveau Règlement l'impose à toutes les entreprises.
La notification à l'autorité de contrôle est obligatoire à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Elle doit se faire dans les meilleurs délais et au plus tard dans les 72 heures après la prise de connaissance de la faille.

Affirmation n° 10: L'obligation d'avoir un Délégué à la Protection des Données ne dépend pas de la taille de l'entreprise

Vrai

L'obligation d'avoir un délégué à la protection des données ne dépend pas de la taille de l'entreprise, mais de son activité.
Lorsque l'activité de base d'une entreprise consiste en des opérations de traitement impliquant « *un suivi régulier et systématique à grande échelle* des personnes concernées » ou le traitement d'une « *quantité à grande échelle de données personnelles sensibles et de données à caractère personnel relatives à des condamnations pénales et à certaines infractions* », l'entreprise doit désigner un délégué à la protection des données.