www.fevad.com

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

www.fevad.com

SRI
LES RÉGIES INTERNET

UDECAM

Règlement Général sur la Protection des données
Tout ce qu'il faut savoir

SOMMAIRE :

Ce document a été réalisé à partir du « General Data Protection Régulation Mythbuster & FAQ » de la Fédération européenne du marketing direct et interactif (FEDMA) dont l'UFMD est membre.

Qu'est-ce que le Règlement général sur la protection des données ?

Le Règlement Général sur la Protection des Données (le « Règlement ») est une nouvelle réglementation de l'UE qui remplacera la Directive 95/46/CE *relative à la protection des personnes*

physiques à l'égard du traitement des données personnelles et à la libre circulation de ces données (la « Directive »). Il est essentiel pour les entreprises de bien le connaître, car il définit les règles pour le traitement des données personnelles, ainsi que les droits des personnes à l'égard de leurs données. Tout manquement à ces règles pourra être sévèrement sanctionné.

Le Règlement sera applicable à la plupart des données utilisées par les acteurs du marketing direct et digital.

Qu'y-a-t-il de nouveau avec le Règlement ?

Le Règlement se fonde sur les principes actuels de la protection des données.
Toutefois, le Règlement est beaucoup plus détaillé que la Directive :

- un champ d'application matériel et géographique plus larges.

Il y a une nouvelle définition plus ample des données personnelles, en conséquence, plus de données vont être concernées par l'application du Règlement (voir Qu'entend-on par données personnelles?). Avec une portée géographique plus large, le Règlement sera également applicable à d'autres organisations en dehors de l'UE (voir A qui s'applique le Règlement ?)

- de nouveaux droits pour les personnes, tel que le droit de portabilité des données, ainsi que de nouvelles obligations pour le traitement des données personnelles, par exemple l'exigence de notification des violations de la sécurité des données, et la réalisation d'analyses afin de déterminer l'impact des nouveaux produits et services sur les droits de protection des données des personnes.

- des dispositions très détaillées, qui s'étendent et clarifient la portée des obligations actuelles pour les entreprises et des droits de protection des données pour les personnes.

Il en est ainsi de :

- l'exigence d'un consentement donné sans ambiguïté,
- l'exigence pour les entreprises de fournir plus d'informations aux particuliers et l'extension du droit à l'effacement des informations personnelles pour les personnes, également appelé droit à l'oubli.

- Application directe dans les Etats membres : Contrairement à une directive qui fixe des objectifs pour les États membres et exige des mesures nationales pour transposer le texte en loi nationale, un règlement est directement applicable dans tous les États membres de l'Union européenne (sans que cela passe par une transposition via une loi au niveau national).

A qui s'applique le Règlement ?

Le Règlement concerne :

- Les entreprises basées dans l'Union européenne, même si le traitement des données a lieu en dehors de l'Union européenne, ou si les données personnelles ne concernent pas des personnes vivant dans l'Union européenne.

- Les entreprises non basées dans l'Union européenne, si le traitement des données personnelles, relatif à des personnes qui se trouvent sur le territoire de l'Union européenne, est lié à l'offre de biens et services (y compris les biens et services gratuits), où au suivi de leurs comportements.

Que dois-je faire?

À partir de la publication du Règlement au Journal officiel de l'Union européenne, les entreprises ont 2 ans pour mettre en œuvre la nouvelle législation.
L'entrée en vigueur du Règlement est prévue pour le deuxième trimestre de 2018. Il est conseillé de démarrer le processus de mise en conformité le plus tôt possible.
Les nouvelles obligations juridiques prévues par le Règlement devront être mises en œuvre et devenir des pratiques communes.
Le processus de mise en œuvre devra comprendre :
- La révision et la mise à jour des politiques de confidentialité, ainsi que des termes et conditions générales ;
- La mise en place de nouvelles procédures techniques et administratives, telle que les exigences de notification de violation des données ;
- La révision des normes de sécurité des données déjà en place ;
- La révision des contrats de traitement de données et autres accords passés avec les partenaires et clients ;
- La révision du cadre juridique pour les transferts internationaux de données vers des pays en dehors de l'Union européenne.

Le nouveau Règlement introduit également la notion de responsabilité (accountability) qui oblige les entreprises à être en mesure de démontrer aux autorités nationales de protection des données qu'elles sont en conformité avec les exigences légales.
Ce concept se traduit par un certain nombre d'obligations, telles que:
- La mise en place des principes de protection des données dès la conception et de protection des données par défaut.
- L'obligation de documenter les politiques et procédures de protection des données.

Qu'entend-on par données personnelles?

Le Règlement définit les données personnelles comme *« toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée"); est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale*; »
Selon le Règlement, certains types de données « en ligne » peuvent être personnels, tels que les identifiants en ligne, les données de localisation, et le numéro d'identification : identifiants de terminaux, cookies, adresses IP...).

À la lumière de la nouvelle rédaction du Règlement, il est nécessaire de procéder à une analyse juridique pour savoir si les données traitées dans l'écosystème numérique sont ou non des données personnelles. Il faudra examiner avec quel niveau de précision, les identifiants utilisés pour distinguer les navigateurs et les terminaux, qui permettent d'identifier une personne en tant que membre d'un groupe de personnes ayant les mêmes intérêts, mais qui en réalité ne permettent pas de l'identifier en tant que personne physique, entrent dans la définition en tant qu'information identifiante.
Par exemple, les adresses IP permanentes détenues par un fournisseur de services Internet sont des données personnelles, dès lors qu'elles permettent d'identifier une personne.

Qu'est-ce que la « pseudonymisation » des données personnelles?

Le Règlement introduit le nouveau concept de « pseudonymisation », qui est un *traitement de données à caractère personnel opéré de façon à ce que les données ne puissent plus être attribuées à une personne concernée sans avoir recours à des informations supplémentaires.*
Cela consiste à soumettre des données personnelles à certaines techniques de confidentialité et de sécurité plus fortes (par exemple, le hachage à sens unique) de telle sorte que l'ensemble de données résultant de ce procédé ne permette plus d'identifier une personne.
Traiter des données pseudonymisées réduit le risque de violation de la vie privée.
Bien qu'il s'agisse toujours d'une forme de donnée à caractère personnel, les données pseudonymisées bénéficieront d'une plus grande flexibilité dans le cadre du Règlement, par exemple pour effectuer du profilage.

Quels sont les principes de la protection des données?

Le Règlement définit les principes du traitement de données personnelles. Ils sont très semblables à ceux énumérés dans la Directive.
Les données personnelles doivent être :
- Traitées de manière licite, loyale et transparente pour les personnes ; (licéité, loyauté, transparence)
- Collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces mêmes finalités ; (limitation des finalités)
- Adéquates, pertinentes et limitées à ce qui est nécessaire par rapport aux finalités pour lesquelles elles sont traitées (minimisation des données)
- Exactes et tenues à jour (exactitude)
- Conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont traitées (limitation de la conservation)
- Traitées de façons à garantir une sécurité appropriée des données à caractère personnel (intégrité et confidentialité)

Dans quel cas peut-on collecter et traiter les données personnelles?

Afin de collecter et de traiter des données personnelles, le traitement doit se fonder sur un

motif de licéité décrit dans le Règlement. Le Règlement en vise 6 comme la Directive.
Ces fondements sont les suivants :
- Le consentement de la personne concernée
- L'exécution d'un contrat auquel la personne concernée est partie
- Le respect des obligations juridiques imposées par la législation de L'Union européenne ou des États membres
- La sauvegarde des intérêts vitaux de la personne concernée
- La réalisation d'une mission effectuée dans l'intérêt public ou dans l'exercice de l'autorité publique
- L'intérêt légitime du contrôleur de données ou d'un tiers

En matière de marketing axé sur les données, les motifs juridiques les plus pertinents et utilisés pour le traitement des données personnelles sont le consentement de la personne et l'intérêt légitime poursuivi par le responsable de traitement des données ou un tiers.

Qu'est-ce qu'un consentement valide à la collecte de données personnelles ?

Selon le Règlement, le consentement doit être : libre, spécifique, éclairé et univoque.
Bien que la définition du consentement soit fondée sur les mêmes principes que ceux de la définition de la Directive, le Règlement est plus clair sur ce qui constitue un consentement valide. Les personnes doivent indiquer leur accord, par une déclaration ou par un acte positif clair.

Si le Règlement permet encore une certaine flexibilité sur la façon de recueillir le consentement des personnes, il faut garder à l'esprit que celui-ci est lié à l'obligation d'information imposée par le Règlement qui varie selon que les données personnelles ont été collectées directement auprès des personnes ou non. Ces informations doivent être fournies de façon concise, transparente et intelligible, et être facilement compréhensible, en utilisant un langage clair et simple. Cela est d'autant plus important que la charge de la preuve du consentement repose sur le responsable de traitement.

Par ailleurs, le Règlement renforce la protection des enfants. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant.

Sur quelle base légale peut-on traiter des données à des fins de marketing ?

En vertu du Règlement en matière de traitement de données personnelles, elles peuvent utiliser le fondement de l'intérêt légitime.
Il s'agit d'un fondement juridique issu de la Directive utilisé pour le marketing direct. De la même manière, le Règlement précise également que "*le traitement de données personnelles à des fins de marketing direct peut être considéré comme réalisé pour un intérêt légitime*".

Il faut évaluer l'intérêt de l'entreprise à traiter des données personnelles par rapport aux libertés et droits fondamentaux de la personne. Le but de cette évaluation est de déterminer si les données

personnelles peuvent être traitées sans s'appuyer sur la base du consentement. Comme cela est déjà le cas avec la Directive actuelle, il est probable que ce test d'équilibre soit satisfait en donnant aux personnes le droit de résilier/se désabonner de la prospection commerciale papier au moment de la collecte de données et de vérifier qu'il ne figure pas sur un fichier repoussoir, telle la liste Robinson.

La Directive vie privée et communications électroniques, qui impose l'obtention du consentement de la personne sur les autres canaux électroniques, continue à s'appliquer. Par exemple, l'obtention du consentement de la personne avant de lui envoyer un email marketing. Le Règlement ne modifie pas ces règles spécifiques.

Attention, certaines catégories particulières de données à caractère personnel dans le cadre du Règlement, dénommées données personnelles sensibles, par exemple, des données relatives aux opinions politiques, à l'origine ethnique et à la santé, ne peuvent être traitées qu'après obtention du consentement explicite de la personne concernée.

Quelles informations doivent être fournies aux personnes dont vous avez collecté les données ?

Afin d'accroître la transparence concernant le traitement des données pour les personnes, le Règlement énumère un certain nombre d'éléments d'information que les entreprises doivent fournir aux personnes lors de la collecte de leurs données personnelles.
Les informations devant être fournies à la personne varient selon que les données ont été collectées auprès de la personne ou non.
Les informations doivent être fournies au moment de la collecte des données ou lorsque les données sont divulguées pour la première fois.
Le Règlement exige que ces informations doivent être fournies de façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples.

Les informations devant être fournies sont:
- L'identité et les coordonnées du responsable de traitement,
- Le cas échant les coordonnées du délégué à la protection des données
- Les finalités et le fondement juridique du traitement des données
- Si les données sont traitées sur la base de l'intérêt légitime de l'entreprise, et quel est l'intérêt légitime
- Les destinataires ou catégories de destinataires avec qui les données seront partagées
- Les informations sur le transfert international de données, y compris sur les garanties en place
- La durée pendant laquelle les données seront conservées, ou les critères permettant de déterminer cette durée
- Les informations sur les droits de la personne concernée (droit de rectification, d'effacement, d'opposition et de portabilité)
- Si les données sont traitées sur la base d'un consentement, le droit des personnes de retirer leur consentement
- Le droit d'introduire une réclamation auprès d'une autorité de contrôle
- si la fourniture des données est imposée de manière règlementaire ou contractuelle
- L'existence d'une prise de décision automatisée (profilage)
- Et l'intention d'effectuer un traitement ultérieur des données pour une autre finalité.

Quand l'entreprise ne recueille pas les données personnelles directement auprès des personnes, en plus des informations ci-dessus, la personne doit également être informée de la catégorie des données traitées, et de la source des données, dans un délai raisonnable, mais ne dépassant pas un mois.

Si les données doivent être utilisées à des fins de communication avec la personne, au plus tard au moment de la 1ère communication avec la personne.
Si les informations sont communiquées à un autre destinataire, lorsque les données sont communiquées pour la 1ère fois.

Il est important que la politique de confidentialité et celle relative à la protection des données soient facilement accessibles et mises à jour.
Un lien vers la politique de confidentialité doit être fourni à chaque fois que des données sont recueillies, à partir par exemple des formulaires d'inscription en ligne.

Qu'est-ce que le droit à l'effacement "droit à l'oubli" ?

Le Règlement permet aux personnes de demander l'effacement de leurs données personnelles dans certaines circonstances.
Ce droit à l'effacement, aussi appelé « droit à l'oubli », s'applique seulement dans un nombre limité de situations énumérées à l'article 17 du Règlement.
Les entreprises peuvent ne pas effacer les informations personnelles, notamment pour respecter une obligation légale, par exemple si elles ont besoin de les garder à des fins de tenue de registres pour les comptables, registres fiscaux.

Le droit à l'effacement implique d'être coordonné avec le droit d'opposition à la prospection commerciale.
Les entreprises doivent également déterminer attentivement si oui ou non les données personnelles doivent être effacées ou ajoutées à leur liste repoussoir interne.
Si une personne demande à une entreprise d'effacer ses données personnelles parce qu'elle ne souhaite plus recevoir de prospection commerciale d'une entreprise particulière, alors plutôt que d'effacer les données personnelles de la personne en question, l'entreprise doit ajouter les coordonnées de contact de la personne à son propre fichier repoussoir en interne.
Si l'entreprise efface entièrement les données personnelles d'une personne il y a alors encore un risque qu'elle lui envoie à l'avenir des correspondances de marketing direct, justement ce à quoi la personne s'oppose. Toutefois, si les coordonnées de la personne ont été ajoutées au fichier repoussoir en interne, celle-ci ne devrait plus envoyer de correspondance de marketing direct à l'avenir.

Les entreprises ont également l'obligation de prendre des mesures raisonnables pour informer les tiers à qui les données personnelles d'une personne ont été transmises de la demande d'effacement, si cela est économiquement et techniquement possible. Elles ne sont pas responsables de l'effectivité de l'effacement des données personnelles par les tiers.

Qu'est-ce que le droit à la portabilité des données ?

Le Règlement introduit un nouveau droit pour les personnes : le droit à la portabilité des données.

Ce droit signifie qu'une personne peut récupérer ses données personnelles nécessaires pour passer d'un fournisseur de services à un autre.
À la demande de la personne, l'entreprise doit fournir à cette dernière les *données personnelles la concernant, qu'elle a fournies à l'entreprise*. Les données personnelles doivent être présentées sous un *format structuré, couramment utilisé et lisible par une machine.* En outre, la personne peut demander que ses données personnelles soient transmises directement à une autre entreprise.
Ce droit à la portabilité des données est limité de deux façons:
- Il ne concerne que les données personnelles traitées par des procédés automatisés.
- Il s'applique uniquement lorsque le traitement des données personnelles est basé sur le consentement de l'utilisateur ou pour l'exécution d'un contrat.
En conséquence, le droit à la portabilité des données ne s'applique pas au traitement de données personnelles basé sur le fondement de l'intérêt légitime.

Qu'est-ce que le droit d'opposition (droit de se désabonner / désinscrire) ?

Le Règlement prévoit pour les personnes un droit d'opposition au traitement de ses données, de se désabonner/désactiver l'exploitation de ses données.
Ce droit existe déjà dans la Directive actuelle.

Lorsque des données personnelles sont utilisées à des fins de prospection, la personne concernée dispose d'un droit d'opposition spécifique à la prospection, qui impose aux entreprises de ne plus traiter ses données à ces fins. Cela peut se traduire par l'inscription de la personne sur une liste repoussoir.
Le Règlement précise que ce droit d'opposition s'applique également aux activités de profilage aux fins de marketing direct.

Les entreprises doivent informer les personnes de leur droit d'opposition au traitement de leurs données de manière explicite et séparée des autres informations que les entreprises se doivent de fournir aux personnes.

Quelles sont les nouvelles règles en matière de Profilage (ciblage)?

Le Règlement définit le profilage comme « *toute forme de traitement automatisé de données à caractère personnel, consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels d'un individu, en particulier, en cas de prévision ou d'analyse des aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique*. »

Dans un contexte de marketing axé sur les données, l'utilisation d'un algorithme d'analyse de données en vue d'évaluer l'intérêt des personnes pour un certain type de produit ou de service, la probabilité pour une personne d'acheter un certain produit, de se comporter d'une certaine manière, ou d'être à un certain endroit, est considéré comme du profilage.

Le Règlement inscrit le profilage dans le cadre d'une décision individuelle automatisée.

Le principe inclut dans la Directive reste identique : donner la possibilité à une personne de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, *produisant des effets juridiques ou l'affectant de manière significative.*

Lorsqu'une entreprise se livre à des activités de profilage autres que pour des fins de marketing direct, elle doit donc estimer l'impact qu'une décision fondée sur le profilage peut avoir sur la personne concernée.
Si la/les décision(s) basée(s) sur le profilage engendre(nt) un *« effet juridique*» ou « *affecte de manière significative* » la personne, cette dernière a le droit de s'opposer au profilage.
Le Règlement identifie clairement le rejet automatique d'une demande de crédit en ligne ou des pratiques de recrutement en ligne sans aucune intervention humaine, comme ayant un effet juridique ou affectant de manière significative les personnes.

Cependant, la personne ne dispose pas de ce droit si :
- le profilage est nécessaire pour la conclusion ou à l'exécution d'un contrat avec la personne concernée
- le profilage est autorisé par la législation européenne ou d'un État membre
- la personne a donné son consentement explicite au profilage

Quelles sont les nouvelles formalités préalables imposées par le Règlement ? Analyse d'impact et consultation préalable

Avant de commencer tout traitement de données personnelles d'une personne, l'entreprise doit déterminer si le traitement est susceptible de créer un risque élevé eu égard à la protection des données des personnes.
Si tel est le cas une analyse de l'impact des opérations de traitement envisagée sur la protection des données à caractère personnel doit être réalisée.
Le Règlement précise que le profilage ayant un effet juridique sur les personnes, ainsi que le traitement à grande échelle des catégories particulières de données (données personnelles sensibles) sont considérés comme traitement à haut risque et nécessitent donc une analyse de l'impact sur la vie privée.
Les autorités nationales de protection des données élaboreront une liste des opérations de traitement pour lesquelles une analyse d'impact est requise.
Le Règlement prévoit une liste d'éléments devant être pris en compte lors de l'analyse d'impact :
- Une description systématique du traitement de données envisagé, des finalités et le cas échéant de l'intérêt légitime ;
- Une évaluation de la nécessité et la proportionnalité du traitement des données au regard des finalités
- Une évaluation des risques pour les droits et libertés des personnes concernées
- Les mesures envisagées pour faire face aux risques, telles les mesures de sécurité supplémentaires pour protéger les données personnelles.

Si l'analyse révèle que le traitement présenterait un risque élevé, une consultation préalable de l'autorité de protection des données avant d'entamer tout traitement.
L'autorité nationale de protection des données fournira par écrit un avis dans un délai de 8 semaines à compter de la réception de la demande de consultation.

Quelles sont les exigences pour un Délégué à la Protection des Données

Le Règlement introduit l'obligation pour certaines entreprises de nommer un Délégué à la Protection des Données.

Lorsque l'activité de base du responsable de l'entreprise « *consiste en des opérations de traitement qui du fait de leur nature, portée ou finalités, exigent un suivi régulier et systématique des données personnelles à grande échelle* » ou « *un traitement à grande échelle des catégories particulières de données* (données personnelles sensibles), la désignation d'un délégué à la protection des données est obligatoire.

Le Délégué doit avoir une connaissance approfondie du droit et des pratiques de la protection des données.

Les entreprises peuvent opter pour un délégué interne ou externe (consultant, cabinets d'avocats).

Le délégué doit avoir à sa disposition les ressources nécessaires pour mener à bien ces tâches et transmet un rapport directement au niveau de direction le plus élevé de l'entreprise.

Il sera chargé de veiller au respect du Règlement, et des autres dispositions du droit visant la protection des données, de conseiller l'entreprise sur ses obligations conformément au Règlement, conseiller sur la fréquence de l'analyse d'impact et la façon dont celle-ci doit être réalisée, et être le contact privilégié de l'entreprise pour les autorités de protection des données nationales et les demandes d'accès aux données personnelles émises par les personnes.

Même si une entreprise n'a pas à nommer un délégué à la protection des données en vertu du Règlement, elle peut volontairement décider d'en nommer un pour l'aider à respecter les obligations imposées par le Règlement.

Qu'est-ce que le "guichet unique" ?

Le concept *de Guichet unique* permet à une entreprise établie dans plus d'un État membre, d'avoir une autorité de protection des données nationales principale avec laquelle elle traitera prioritairement.

Par exemple, si les activités de marketing d'une entreprise paneuropéenne sont réalisées à partir du Royaume-Uni, l'autorité nationale de protection des données du Royaume-Uni sera l'autorité principale pour les activités de marketing de cette entreprise. Si l'entreprise basée au Royaume-Uni a fait de la prospection commerciale à un citoyen français et que ce même citoyen français estime que cette action constitue une violation au Règlement, alors ce citoyen français doit déposer une plainte à l'autorité nationale de protection des données en France. L'autorité nationale de protection des données en France doit transmettre la plainte à l'autorité nationale de protection des données au Royaume-Uni. La décision finale serait prise par l'autorité nationale de protection des données au Royaume-Uni après avoir consulté l'autorité nationale de protection des données en France.

Si la plainte est liée à un point de droit plus vaste en vertu du Règlement, l'autorité nationale de protection des données au Royaume-Uni peut renvoyer la plainte au comité européen à la protection des données, composée de représentants de toutes les autorités nationales de protection des données nationales.

Il existe une procédure complexe qui permet la consultation entre les autres autorités nationales de protection des données et le comité européen des données, en cas de désaccords entre les

autorités de protection des données nationales, appelée mécanisme de cohérence.

Quelles sont les nouvelles règles pour le transfert international de données ?

Tout comme la Directive, le Règlement autorise les transferts internationaux de données vers des pays en dehors de l'Union européenne lorsque le pays destinataire prévoit un niveau de protection adéquat.
La Commission européenne a le pouvoir de décider si un pays en dehors de l'Union européenne prévoit ou non une protection adéquate. La Commission européenne sera également en mesure de déclarer l'adéquation *d'un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers.*

En l'absence d'une décision d'adéquation, le Règlement autorise les transferts internationaux de données sur la base de garanties appropriées et *à condition que les personnes concernées disposent de droits opposables et de voies de droit effectives.*
Le Règlement reconnaît sur cette base plusieurs outils pour les transferts internationaux de données vers des pays en dehors de l'Union européenne:
- Les règles d'entreprise contraignantes, qui nécessitent l'approbation des autorités nationales de protection des données. Elles seront privilégiées par les grandes entreprises dans la mesure où le processus d'approbation est juridiquement et administrativement complexe et long.
- Les clauses types de protection des données, aussi appelées clauses contractuelles types. Elles remplacent les modèles de clauses contractuelles en vertu de la Directive. La Commission comme les autorités de contrôle peuvent élaborer des clauses contractuelles type.
- Un code de conduite approuvé ou un mécanisme de certification approuvé avec des engagements contraignants et exécutoires pris dans le pays tiers, d'appliquer les garanties appropriées.

En l'absence de décision de la Commission européenne d'adéquation ou de garanties appropriées, une entreprise peut encore transférer des données personnelles à une entreprise dans un pays hors de l'UE sous certaines conditions, notamment si :
- la personne a donné son consentement explicite, après avoir été informée des risques que peut comporter le transfert pour ses droits.
- le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et l'entreprise ou à la mise en œuvre de mesures précontractuelles à la demande de la personne.
- le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu entre l'entreprise et une autre personne physique ou morale.
- le transfert est nécessaire pour des motifs importants d'intérêt public;
- le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice;
- le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement;

- le transfert a lieu au départ d'un registre qui, conformément au droit de l'Union ou au droit d'un État membre, est destiné à fournir des informations au public et est ouvert à la consultation du

public en général ou de toute personne justifiant d'un intérêt légitime, mais uniquement dans la mesure où les conditions prévues pour la consultation dans le droit de l'Union ou le droit de l'État membre sont remplies dans le cas d'espèce.

En dehors de ces cas, un transfert vers un pays tiers ne peut avoir lieu que si ce transfert ne revêt pas de caractère répétitif, ne concerne qu'un nombre limité de personne et est nécessaire aux fins des intérêts légitimes impérieux de l'entreprise sans qu'ils ne prévalent sur les intérêts droit et libertés de la personne concernée et que des garanties appropriées aient été mises en place. En outre, lors du transfert de données sur une telle base, l'entreprise basée UE devra informer son autorité nationale de protection des données du transfert.

Quelles sont les nouvelles obligations en matière de sécurité des données?

Le Règlement contient des exigences quant à la sécurité des données semblables à celles de la Directive actuelle.

Ainsi les entreprises et leurs prestataires de services extérieurs « *doivent mettre en œuvre des mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adapté au risque* ".

Le Règlement permet aux entreprises de prendre en considération l'*état de l'art et les coûts de mise en œuvre*, ainsi qu'un certain nombre d'aspects liés au traitement des données lui-même, dans le cadre de l'approche fondée sur le risque, lors de l'évaluation des mesures de sécurité nécessaires à mettre en place. Comme cela est le cas sous la Directive actuelle, les entreprises doivent mettre en place des mesures de sécurité pour protéger le traitement des données personnelles. Ces mesures de sécurité doivent être proportionnées au niveau de risque que le traitement des données peut comporter pour les particuliers concernés.

Le Règlement suggère l'utilisation d'un certain nombre de mesures de sécurité, y compris :

- La pseudonymisation et le chiffrement des données personnelles
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience en constante des systèmes et services de traitement de données personnelles
- des moyens permettant de rétablir la disponibilité et l'accès aux données personnelles dans des délais appropriés en cas d'incident physique ou technique
- une procédure visant à tester, à analyser, et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement des données personnelles.

L'approche du Règlement en matière de sécurité est liée aux nouvelles obligations, à savoir, garantir les principes de protection des données dès la conception et de protection des données par défaut (privacy by design, by défault), et veiller à ce que l'impact des nouveaux projets sur les droits de protection des données des personnes soit évalué (analyse d'impact).

Le respect des obligations de sécurité repose tant sur l'entreprise que ses sous-traitants.

Quelles sont les nouvelles sanctions en cas de violation des données?

Le Règlement propose une définition assez large de la violation de données :
une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données;
Cette définition ne prend pas en considération si la violation crée un préjudice pour la personne.

En cas de violation de la sécurité des données, les entreprises doivent informer leur autorité nationale de protection des données dans les meilleurs délais, ou au plus tard 72 heures après la découverte de celle-ci, à moins que la violation ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.
Si l'entreprise ne signale pas la violation de la sécurité des données à l'autorité nationale de protection des données dans ce délai, elle doit expliquer les raisons pour lesquelles le délai a été dépassé une fois la violation signalée.
La notification doit décrire de façon claire et simple la nature de la violation de données personnelles et comprendre certains éléments d'information :
- le nom et les coordonnées du Délégué à la Protection des Données ou d'un autre contact auprès duquel il est possible d'obtenir plus d'informations sur la violation
- les conséquences probables de la violation des données personnelles
- décrire les mesures que l'entreprise a prises ou qu'elle se propose de prendre pour remédier à la violation de la sécurité des données, y compris le cas échéant, des mesures prises pour réduire l'impact négatif éventuel de la violation.
Si la violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, l'entreprise doit communiquer la violation à la personne concernée dans les meilleurs délais.
Toutefois, l'entreprise est exemptée de l'obligation de notification si :
- elle a mis en place des mesures de protection techniques et organisationnelles appropriées pour protéger les données personnelles, telles que le cryptage, et que ces dernières ont été appliquées aux données affectées par la violation.
- elle a pris des mesures ultérieures qui garantissent que le risque élevé n'est plus susceptible de se matérialiser,
- Informer la personne implique des efforts disproportionnés. Dans ce cas une communication publique ou mesure similaire peut être faite.

Qu'entend-on par principe de responsabilité?

Le nouveau Règlement introduit le principe de responsabilité obligeant les entreprises à être en mesure de démontrer aux autorités nationales de protection des données qu'elles se conforment aux dispositions du Règlement.
Malgré la suppression des obligations déclaratives auprès de l'autorité de protection des données nationale pertinente, les entreprises devront toujours, en vertu du Règlement, conserver les copies des informations qu'elles auraient précédemment envoyées à l'autorité nationale de protection des données dans le cadre d'une procédure déclarative ou d'autorisation.
L'autorité nationale de protection des données peut exiger l'accès à ces informations à tout moment.