



FEDERATION EUROPEENNE DE MARKETING DIRECT

**CODE DE DEONTOLOGIE EUROPEEN
EN MATIERE D'UTILISATION DE DONNEES A CARACTERE PERSONNEL
DANS LE MARKETING DIRECT**

MEMORANDUM EXPLICATIF

La FEDMA représente le secteur du marketing direct à l'échelon européen. Ses membres nationaux regroupent les Associations de Marketing Direct (DMA) de 12+ pays de l'Union européenne (à l'exception de la Belgique, du Luxembourg et du Danemark) ainsi que de la Suisse, de la Norvège, de la Hongrie, de la Pologne et des Républiques tchèques et slovaques. Ces associations représentent les utilisateurs, les prestataires de services et les annonceurs du marketing direct. La FEDMA comprend également 350 entreprises directement affiliées.

La FEDMA représente directement ou indirectement, par le biais d'associations professionnelles, quelque 10.000 professionnels du marketing direct en Europe, ce qui place la FEDMA dans une situation idéale pour rédiger un code de déontologie européen sur la protection des données à l'intention de ces professionnels et dont l'élaboration résulte des discussions du groupe de travail prévu par l'article 29. Cet instrument essentiel se veut une interprétation de la directive européenne relative à la protection des données dans des termes intelligibles par les professionnels du marketing direct. Dans le cas où la pratique dépasse déjà le niveau de protection de la directive, ou le FEDMA recommande qu'un niveau de protection plus élevé serait souhaitable, des règles plus exigeantes ont été incorporées dans le code.

Tous les membres nationaux de la FEDMA, c'est à dire les associations professionnelles, se sont engagées à ce que leurs propres codes de déontologie nationaux offrent à tous les égards un niveau de protection des personnes concernées au moins aussi élevé que celui prévu par le code de la FEDMA, étant précisé que les codes nationaux pourront prévoir des normes encore plus strictes lorsque les législations nationales ou les exigences d'autorégulation les permettent ou les contraignent.

Ce code se veut avant tout un instrument de bonnes pratiques (« best practices ») et doit être utilisé comme un document de référence dans le cadre des législations applicables. Les membres directs de la FEDMA respecteront les normes établies par le code de la FEDMA, sous réserve cependant de toujours se conformer aux législations nationales ou aux dispositions d'autorégulation applicables.

La FEDMA espère et promulguera activement le code de la FEDMA pour qu'il soit considéré par l'ensemble des professionnels du marketing direct en Europe, membres ou non, comme la norme de référence ou le code de déontologie général de l'ensemble de la profession.

La FEDMA reconnaît également que ce code de déontologie ne constitue que la première étape du développement continu de bonnes pratiques (« best practices ») effectives dans le domaine de la protection des données. Les améliorations qui seront apportées aux éditions subséquentes de ce code auront vocation à refléter les aspirations croissantes des professionnels responsables et devraient permettre une évolution progressive des pratiques de la profession à travers des frontières, conformément aux attentes constantes et légitimes de sa clientèle.

Il convient de préciser que les différents moyens de communication utilisés par le Marketing direct ont fait l'objet de plusieurs réglementations : les directives 97/66/ec (télécommunications et protection des données) et 97/7/EC (vente à distance) requièrent le consentement de la personne concernée avant l'envoi de

communications commerciales par fax ou automate d'appel. En outre, la directive 2002/58/EC (protection des données et communication électronique) prévoit que le consentement est nécessaire avant l'utilisation de communications électroniques (par exemple, le e-mailing) à destination des consommateurs n'ayant pas de relations préalables avec le responsable du traitement.

Il est important de rappeler que la législation en matière de protection des données s'applique au traitement des données à caractère personnel et ce quel que soit le moyen utilisé.

Ce code devra être lu en conjonction avec les autres codes de déontologie existants et à venir de la FEDMA, y compris les principes européens gouvernant l'utilisation du téléphone en tant qu'outil de marketing par les entreprises et le code de conduite européen. Ce code devra également tenir compte des conventions globales sur les services MPS et TPS ainsi que des principes du Global E-mail Preference Service¹.

Ce code de déontologie en matière d'utilisation des données à caractère personnel a été conçu à l'intention des professionnels du marketing direct de l'Union européenne ainsi que des pays qui n'appartiennent pas à l'Union européenne², mais dont les législations nationales de protection des données sont alignées sur la directive européenne.

Toutes les dispositions de ce code s'appliquent sous réserve des dispositions prévues dans les lois nationales applicables. Dans la mesure où des règles spécifiques existent au niveau national, ces dernières devront être satisfaites conformément aux règles relatives à la loi applicable telles que décrites dans ce code et conformément à la législation communautaire.

1 Les conventions globales sur les Preference Services, le code de conduite de la FEDMA en matière de commerce électronique et les principes européens sur l'utilisation du téléphone en tant qu'outil de marketing par les entreprises sont disponibles auprès de la FEDMA. Pour de plus amples informations sur le Global E-mail Preference Service, voir <http://www.e-mps.org>. Les listes Robinson sont l'équivalent des Preference Services (voir note en bas de la page 11).

2 Les pays de l'EEE et les autres pays européens dont les législations nationales de protection des données offrent un niveau de protection adéquat.

DEFINITIONS

MARKETING DIRECT

La communication par quel moyen que ce soit (comprenant de manière non limitative le courrier, la télécopie, le téléphone, les services en ligne, etc.) de toute offre de publicité ou marketing, qui est réalisée par le professionnel même ou sous sa responsabilité et qui s'adresse à des particuliers.

DONNEES A CARACTERE PERSONNEL

On entend par données à caractère personnel toute information concernant une personne physique identifiée ou identifiable. Est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

Nota

On entend par données à caractère personnel toute information concernant une personne, qui est conservée sous une forme permettant d'identifier la personne concernée, et qui peut par exemple se réduire au nom de famille. Certaines informations ne contenant pas de nom de famille doivent cependant être considérées comme des données à caractère personnel et sont, par conséquent, couvertes par ce code. Cela pourra par exemple être le cas d'une adresse postale, d'un numéro de téléphone ou de télécopie, d'une adresse électronique ou d'une fonction, si la personne à laquelle ces données se rapportent peut, de manière raisonnable, être identifiée.

DONNEES SENSIBLES

Toutes les données qui divulguent les informations suivantes relatives à une personne concernée sont sensibles et sont soumises à des restrictions au niveau de leur traitement :

- Origine raciale ou ethnique ;
- Opinions politiques ;
- Appartenance à un syndicat ;
- Croyances religieuses ou philosophiques ;
- Santé physique ou psychique ;
- Vie sexuelle ;
- Les infractions, condamnations pénales et mesures de sécurité.

PROFESSIONNEL DU MARKETING DIRECT

Toute personne physique ou morale (y compris les associations à but caritatif et les partis politiques) qui communique par quel moyen que ce soit (comprenant de manière non limitative le courrier, la télécopie, le téléphone, les services en ligne, etc.) toute offre de publicité ou marketing qui est adressé à des particuliers.

PERSONNE CONCERNEE

La personne par rapport à laquelle les données à caractère personnel pourront être identifiées ou pourront être identifiables.

COORDINATEUR CHARGE DE LA PROTECTION DES DONNEES

Toute personne physique nommée par les responsables de traitements afin d'exécuter les fonctions décrites dans ce code.

RESPONSABLES DE TRAITEMENTS

Dans le cadre de ce code, le terme « responsable de traitement » désignera toute personne physique ou morale qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel.

Nota

On évitera toute confusion entre le responsable du traitement et le propriétaire des données. Une personne pourra, par exemple, être à la fois propriétaire d'une base de données (dans la mesure où cette personne physique ou morale détient les droits d'utiliser cette base de données) et parallèlement responsable de traitement de ces données. Toutefois la qualité de propriétaire et de responsable de traitement ne sont pas toujours liées. Le responsable du traitement n'est pas nécessairement propriétaire des données.

SOUS-TRAITANT

Toute personne physique ou morale, autre qu'un employé des responsables de traitements, qui traite les données à caractère personnel pour le compte des responsables de traitements, conformément aux instructions de ce dernier et sous sa responsabilité.

TIERS

Toute personne physique ou morale, qui n'est ni le responsable de traitement, ni le sous-traitant ni un agent/employé du responsable de traitements ou du sous-traitant.

Nota

Les responsables de traitements pourront, par exemple, nommer la société A comme sous-traitant. Le sous-traitant pourra uniquement traiter les données conformément aux instructions des responsables de traitements. Si les responsables de traitements décident cependant de louer une liste spécifique à une société B, cette société sera un tiers.

TRAITEMENT

Dans le cadre de ce code, le traitement désigne toute opération automatisée appliquée à des données à caractère personnel à des fins de marketing direct. Les opérations manuelles sont également concernées lorsque celles-ci sont exécutées de manière structurée selon des critères spécifiques afin de faciliter l'accès à ces données.

Nota

Ce terme couvre toutes les étapes individuelles de la chaîne d'opérations qu'une organisation pourra effectuer à l'égard des données à caractère personnel, depuis leur collecte initiale jusqu'à leur destruction, y compris toutes les opérations intermédiaires telles que leur rectification, leur détention et leur communication. Ce code ne s'applique qu'au traitement relatif aux activités de marketing direct. Les professionnels devront également s'assurer que les autres types de traitement qu'ils effectuent sont par ailleurs conformes aux règles applicables en matière de protection des données.

COMMUNICATION

Toute communication (fourniture ou mise à disposition) de données à caractère personnel (par ex. location, vente) à des tiers.

ENFANTS

Toute personne âgée de moins de 14 ans, sauf définition contraire dans les législations/autorégulations nationales.

PARENT

Le parent de l'enfant ou son tuteur.

1 Droit applicable

1.1 Professionnels du marketing direct établis dans un territoire de l'Union européenne/l'EEE

Le professionnel qui est établi dans le territoire de l'Union européenne/l'EEE et qui souhaite connaître la législation nationale applicable, doit tenir compte des règles suivantes :

- 1.1.1 Si le professionnel est établi dans un seul pays de l'Union européenne/l'EEE et n'a par conséquent qu'un seul responsable du traitement, la loi applicable sera celle du pays dans lequel le responsable du traitement est établi, sous réserve des règles énoncées au point 1.1.4.
- 1.1.2 Si le professionnel est établi dans plusieurs Etats membres de l'Union européenne/l'EEE et si l'un, et seulement l'un de ces établissements, est considéré comme le responsable du traitement, alors que les autres établissements ne sont que des sous-traitants, dans ce cas chaque sous-traitant devra respecter la loi nationale du responsable du traitement, sauf en ce qui concerne les mesures de sécurité, pour lesquelles le sous-traitant devra observer sa propre législation nationale.
- 1.1.3 Si le professionnel est établi dans plusieurs Etats membres de l'Union européenne/l'EEE et si chacun d'entre eux agit comme responsable de traitements, alors chaque établissement devra respecter la loi nationale du pays dans lequel il est établi.
- 1.1.4 Si le **professionnel agit en tant que responsable de traitements** et recourt à un sous-traitant implanté dans un Etat membre différent de l'Union européenne/l'EEE, ce sous-traitant devra appliquer les lois applicables aux responsables de traitements établis dans l'Union européenne, à l'exception des dispositions relatives aux mesures de sécurité. Pour ce dernier cas, la législation du pays dans lequel le sous-traitant est établi s'appliquera.
- 1.1.5 Le fait que les données proviennent de personnes physiques appartenant à un ou plusieurs pays de l'Union européenne/l'EEE ou à des pays qui ne font pas partie de l'Union européenne/l'EEE ne constitue pas un critère déterminant pour désigner la loi applicable.

Le tableau suivant résume, pour des raisons de commodité, les différents cas de figure possibles :

CAS	FAITS				LOI APPLICABLE	
	Professionnel du MD établi en	Responsable de traitements établi en	Sous-traitant établi en	Provenance des données	Traitement respectif	Mesures de sécurité
1	BE	BE	BE	UE EEE US	BE	BE
2	BE NL UK	BE	NL UK	UE EEE US	BE	NL UK
3	BE	BE NL UK	FR	UE EEE US	BE NL UK	FR
4	BE	BE NL UK	SP PT LUX	UE EEE US	BE NL UK	SP PT LUX

1.2 Responsables de traitements établis en dehors du territoire de l'Union européenne/l'EEE.

Tout responsable de traitements qui n'est pas établi dans l'Union européenne/l'EEE, ou dans un pays tiers disposant d'un niveau de protection adéquat et qui n'offre pas de mécanisme de protection reconnue par l'Union Européenne devra respecter la loi nationale de l'un des Etats membres de l'Union européenne/l'EEE dès lors qu'il utilise, à des fins de traitement des données, un équipement situé dans l'un de ces Etats membres (par exemple un centre d'appels pour recueillir les données à caractère personnel, un bureau de traitement chargé de traiter les données à caractère personnel pour son compte, un courtier en fichiers pour mettre à jour ses listes, etc.). Dans ce cas :

- 1.2.1 Le responsable du traitement désignera un représentant (une personne physique ou morale) qui sera établi dans l'Etat membre dans lequel le traitement a lieu. Le représentant sera chargé de garantir, vis-à-vis des autorités nationales compétentes, le respect de la législation nationale applicable par le responsable du traitement. (Ce qui ne signifie pas que les autorités ne pourront pas intenter d'actions en justice à l'encontre du responsable du traitement).
- 1.2.2 La législation applicable sera celle du pays dans lequel le représentant est établi.
- 1.2.3 Les dispositions de l'article 1.2 **ne s'appliquent pas** si l'équipement est uniquement utilisé à des fins de transit sur le territoire de l'Union européenne/l'EEE (par exemple, si le responsable de traitement est établi au Canada, les données pourront être recueillies dans des pays n'appartenant pas à l'Union européenne/l'EEE, puis envoyées au Canada par le biais d'un prestataire de services de télécommunications britannique).

2 Collecte de données à caractère personnel

2.1 Collecter des données directement auprès de la personne concernée

Les responsables de traitements devront s'assurer que les données sont collectées de manière loyale et que le droit à l'information de la personne concernée, tel qu'il est défini dans ce code, est respecté.

Principes généraux en matière de traitement loyal

- *Informations essentielles*

Les responsables de traitements doivent s'assurer que les personnes concernées sont informées :

- de l'identité des responsables de traitements (par ex. nom et adresse) ;
- des finalités du traitement (par ex. finalités commerciales ou promotionnelles)

Ces informations essentielles devront être communiquées au moment de la collecte des données, à moins que les informations découlent de manière parfaitement claire du contexte (par exemple, en ce qui concerne l'identité des responsables de traitements et la finalité, si le nom de la société figure clairement dans la promotion) ou que la personne concernée ne soit déjà en possession de ces informations (par exemple si la personne concernée a conclu un contrat avec la société).

- *Informations sur les droits d'accès et de rectification des données et le droit d'objection*

Les responsables de traitements doivent s'assurer que les personnes concernées sont informées :

- qu'elles ont le droit d'accéder et de rectifier les données erronées qui les concernent ;
- qu'elles ont le droit de ne pas être contactées à des fins de marketing direct ;
- qu'elles ont le droit de s'opposer au traitement de leurs données à caractère personnel à des fins de marketing direct.

Traitement des situations spécifiques

- *Informations dans le cas de données utilisées pour les activités de marketing direct des responsables de traitements.*

Lorsque les données sont destinées aux propres activités de marketing direct des responsables de traitements, ces derniers devront s'assurer que la personne concernée a connaissance de ces informations essentielles et de son droit de s'opposer à une telle utilisation.

Les responsables de traitements devront communiquer ces informations au moment de la collecte et mettre en oeuvre tous leurs efforts pour y parvenir. Au cas où cela s'avèrerait cependant difficile ou impossible (par ex. encarts publicitaires restreints ou télémarketing) et sous réserve que cela soit autorisé par la législation nationale, ces informations devront être communiquées le plus rapidement possible après la collecte, par exemple lors du premier envoi de documents n (facture, reçu, etc.), sous forme écrite ou durable, à la personne concernée.

- *Informations en cas de communication*

Outre ces informations essentielles, lorsque les données sont destinées à des tiers, les responsables de traitements devront s'assurer que les personnes concernées sont informées :

- des destinataires ou types de destinataires des données et de la finalité pour laquelle les données seront communiquées.
- de leur droit de s'opposer à ce que ces données soient divulguées à des fins de marketing direct.

Ces informations devront être communiquées au moment de la collecte des données et tous les efforts devront être consentis en ce sens. Au cas où cela s'avèrerait cependant difficile ou impossible (par ex. encarts publicitaires restreints ou télémarketing) et sous réserve que cela soit autorisé par la législation nationale, ces informations devront être communiquées avant d'effectuer toute communication de ce type à des tiers.

La communication de ces informations peut ne pas être nécessaire lorsque les informations en question ont déjà été communiquées par le biais de mécanismes adéquats (par ex. sous la forme d'un avis collectif approprié généralement accessible et suffisamment ciblé par rapport à un public spécifique). De tels mécanismes doivent cependant être autorisés par la législation nationale applicable et être appliqués conformément aux exigences juridiques contenues dans la législation nationale concernée.

- *Informations en cas d'utilisation de questionnaires et autres formulaires*
Outre ces informations essentielles, les responsables de traitements doivent s'assurer que les personnes concernées sont informées du caractère obligatoire ou volontaire des réponses et des conséquences possibles en cas de non-réponse (A titre d'exemple, et de manière non limitative, dans le cas de non envoi du cadeau dans le cadre d'une collecte de données par voie de questionnaire). Les responsables de traitements devront également s'assurer que les questions posées ont un caractère légitime.

Dans le cas de questionnaires, ces informations devront être communiquées au moment de la collecte.

2.2 Collecte auprès de sources autres que la personne concernée

2.2.1 Lorsque les données à caractère personnel ne sont pas directement collectées auprès des personnes concernées, les responsables de traitements devront prendre les dispositions nécessaires pour s'assurer que les personnes concernées ont néanmoins connaissance des informations qu'elles auraient reçues en cas de contact direct avec les responsables de traitements. Par exemple, les listes louées, les campagnes offre-ami ou les données collectées à partir de questionnaires doivent notamment être conformes aux principes de légitimité tels que définis à l'Article 2.1.

2.2.2 Les responsables de traitement devront communiquer les informations mentionnées à l'Article 2.1 :

- au moment de procéder à l'enregistrement (c'est à dire au traitement) des données,
- ou, lorsque la communication des données à des tiers est envisagée, au plus tard au moment de la communication,

Sauf dans les cas où la personne concernée en est déjà informée.

2.2.3 Par dérogation aux dispositions de l'article 2.2.1 et sous réserve que les données utilisées aient été initialement collectées dans le strict respect des règles relatives à la protection des données, les mesures d'information prévues aux alinéa précédent pourront ne pas être appliquées en cas de circonstances exceptionnelles spécifiques où la communication de telles informations supposerait un effort disproportionné, dès lors que des garanties appropriées supplémentaires, fixées par les législations nationales, sont observées. Parmi les circonstances exceptionnelles, on retiendra en particulier, celles qui impliquent des dépenses disproportionnellement élevées en temps et en argent. Par exemple, quand des données sont obtenues d'un tiers et doivent être utilisées dans un bref délai, il pourra apparaître disproportionné d'en informer immédiatement la personne concernée, alors que cela peut attendre jusqu'à ce que le premier contact ait lieu.

2.2.4 Ces éléments d'appréciation devront toujours être contrebalancés par rapport aux conséquences qui pourraient être subies par les personnes concernées du fait de l'application de cette dérogation. Les circonstances dans lesquelles cette dérogation pourra s'appliquer pourront notamment inclure, les cas suivants:

- Lorsque les données à caractère personnel sont détenues à des fins de verrouillage ou de vérification d'adresse ;
- Lorsque les données à caractère personnel sont effacées via l'application d'une liste Robinson ou d'un fichier Preference Service
- Lorsqu'un professionnel du marketing direct retire ou efface les données à caractère personnel des personnes de la liste de marketing qui ne correspondent pas au profil désiré.

2.2.5 Après avoir évalué les éléments d'appréciation pertinents et avoir décidé d'appliquer cette dérogation, les responsables de traitement devront prévoir une déclaration écrite (justifiant leur décision, le type d'informations que les responsables de traitement devront donner et expliquant en quoi les personnes concernées ne seront pas pénalisées par l'application de la dérogation) et s'assurer que cette déclaration est disponible par la suite pour justifier leur décision.

2.3 Collecte de données sensibles

Compte tenu de l'importance particulière que revêtent les données sensibles par rapport aux droits fondamentaux de la personne concernée en matière de protection de la vie privée, le traitement de telles données devra faire l'objet d'une attention particulière.

Si les données à caractère personnel qui doivent être collectées contiennent des données sensibles, les responsables de traitements devront obtenir le consentement explicite de la personne concernée avant de collecter et de continuer à traiter ces données à caractère personnel. Le consentement explicite devra être spécifique, libre et informé, de sorte qu'il ne puisse-t-il avoir aucun doute quant au consentement de la personne concernée, susceptible de nécessiter une clarification de ce consentement. Un consentement explicite ne doit pas l'être nécessairement par écrit, bien que cela soit souvent le cas dans la pratique dans la mesure où un tel document constitue une preuve efficace de consentement, à moins que :

- les données n'aient été manifestement rendues publiques par la personne concernée (par exemple, dans le cas d'informations provenant d'une source publique telle qu'un annuaire, où il a été donné à la personne concernée la possibilité de ne pas mentionner ces données) ou ;
- les données soient traitées par une organisation à but non lucratif avec une finalité politique, philosophique, religieuse ou syndicale. Si ces organisations traitent les données sans le consentement explicite de la personne concernée, elles devront s'assurer que :
 - le traitement est effectué dans le cadre des activités légitimes de ces organismes
 - des garanties appropriées sont offertes ;
 - le traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers ;
 - le traitement a lieu en rapport avec les objectifs de l'organisme à but non-lucratif ;
 - les données ne sont pas divulguées à des tiers, sans le consentement des personnes concernées.

Ce pourra être par exemple le cas d'une église ou d'une association religieuse qui envoie (ou qui recourt à un sous-traitant pour cet envoi) à ses membres une lettre annonçant la publication d'un bulletin religieux auquel les membres intéressés pourront s'abonner, ou pour recueillir des fonds en vue d'apporter une aide et une assistance dans certaines situations spécifiques.

En aucun cas, les sociétés ne devront utiliser les données sensibles d'une manière qui puisse porter atteinte aux droits fondamentaux et aux libertés de la personne concernée. Les données doivent toujours être traitées dans le cadre d'activités légitimes.

Lorsque les données sensibles recueillies dans le cadre d'activités de marketing direct et sont traitées pour d'autres finalités statistiques ou d'analyses elles doivent être rendues anonyme ou, au moins transformées de manière à ne pas permettre l'identification de l'intéressé, sauf lorsque le responsable du traitement recueille le consentement explicite de la part de la personne concernée.

2.4 Finalités différentes

2.4.1 Si l'on envisage de traiter des données à caractère personnel pour une finalité différente de celle pour laquelle les données ont été à l'origine collectées, les responsables de traitements devront s'assurer, entre autres, que cette nouvelle finalité est compatible avec la finalité déclarée. Si elle l'est, le traitement des données pour cette nouvelle finalité sera autorisé. Dans l'hypothèse où la nouvelle finalité s'avère incompatible avec la finalité déclarée, le nouveau traitement des données ne pourra être effectué que dans la mesure où il interviendra conformément à la législation sur la protection des données applicables.

- 2.4.2 Les responsables de traitements qui évaluent la compatibilité de la nouvelle finalité devront entre autres tenir compte des critères suivants : la nouvelle finalité est-elle fondamentalement différente de la finalité pour laquelle les données ont été collectées ? Les personnes concernées auraient-elles pu raisonnablement le prévoir ou est-il probable qu'elles s'y seraient opposées si elles l'avaient su ? Le responsable du traitement doit toujours tenir compte des recommandations applicables ayant valeur légale émanant des autorités de protection des données compétentes.

2.5 Asiles-mailings

Dans le cas d'asiles-mailings, le responsable du traitement doit être clairement identifiable

Par asiles-mailings, on entend la pratique qui consiste pour un responsable de traitement à joindre une offre d'une tierce partie dans un mailing.

Les critères sélectifs susceptibles d'avoir un effet préjudiciable sur les droits de la personne concernée - par exemple dans le cas d'utilisation de données sensibles liées à des comportements d'achat (rappel achat de produits pharmaceutiques) - ne devront pas être utilisés.

2.6 Dispositions spécifiques concernant les enfants

- 2.6.1 Dans le cadre de la collecte de données relatives à des enfants, les responsables de traitements devront faire tous les efforts raisonnables pour s'assurer que l'enfant et/ou le parent sont correctement informés des finalités du traitement des données relatives à l'enfant. En particulier, en cas d'utilisation de matériel commercial destiné à des enfants ou de toute autre collecte de données sciemment effectuée auprès d'enfants, la notice d'information devra être bien mise en évidence et facilement accessible et compréhensible par des enfants.
- 2.6.2 A chaque fois que la législation nationale ou européenne sur la protection des données applicable exige le consentement de la personne concernée pour le traitement, les responsables de traitements devront obtenir le consentement éclairé et préalable du parent pour le traitement des données relatives à l'enfant concerné. La forme et la méthode selon lesquelles le consentement devra être obtenu devront être toujours conformes aux lois et aux règles d'autorégulation applicables.
- 2.6.3 Les responsables de traitements donneront au parent de l'enfant les mêmes droits sur les données des enfants que ceux décrits à la section 3.5 de ce code. Les responsables de traitements devront faire tous les efforts raisonnables afin de s'assurer que la personne qui exerce les droits de l'enfant est le parent de l'enfant.
- 2.6.4 Les responsables de traitements ne devront pas demander à l'enfant, en échange de sa participation à un jeu, d'un prix ou dans le cadre de toute autre activité liée à des avantages promotionnels, de divulguer plus de données à caractère personnel qu'il n'est strictement nécessaire pour la participation à une telle activité.

3 Responsabilités des responsables de traitements

3.1 Principes de protection des données

3.1.1 Les responsables de traitements doivent se conformer aux principes suivants : les données à caractère personnel doivent être :

- traitées loyalement et légalement pour des raisons légitimes (conformément aux lois applicables et aux dispositions de ce code) ;
- collectées pour une finalité spécifiée, explicite et légitime (par ex. finalités déclarées aux autorités de protection des données telles que la fourniture d'informations personnelles, les activités de vente à distance) ;
- ne pas être traitées ultérieurement de manière incompatible avec ces finalités³ à moins que la personne concernée n'y ait également consenti ;
- adéquates, pertinentes (par ex. il est normal pour une compagnie aérienne de demander à ses passagers quelles sont leurs habitudes alimentaires en vue de leur proposer les repas qu'ils souhaitent, alors qu'une société de location de voitures n'a pas besoin de connaître les habitudes alimentaires de ses clients dans la mesure où elle ne leur fournit normalement pas de repas) et ne pas être excessives par rapport aux finalités pour lesquelles elles sont collectées et/ou traitées ultérieurement ;
- exactes et mises à jour. On utilisera pour ce faire des listes d'opposition (internes et listes Robinson générales⁴), les données se trouvant dans le domaine public et le droit à la rectification exercée par la personne concernée.
- conservées dans un format qui permet d'identifier les personnes concernées, mais seulement pendant la période nécessaire aux fins pour lesquelles les données ont été collectées et pour lesquelles elles sont traitées.

3.1.2 Les responsables de traitements devront passer un contrat avec leurs sous-traitants dans lequel le sous-traitant s'engage à se conformer à ces principes et à agir uniquement selon les instructions des responsables de traitements. Il incombe en dernier lieu aux responsables de traitements de s'assurer que le traitement se déroule de manière loyale et légale et cette responsabilité ne peut être transférée au sous-traitant par le biais d'un contrat.

3.2 Déclaration aux autorités de protection des données

Les responsables de traitements devront s'assurer que leurs activités de traitement sont enregistrées conformément à la législation pertinente applicable.

3.3 Mesures de sécurité

3.3.1 Les responsables de traitements devront s'assurer que des mesures de sécurité appropriées sont adoptées, tenant compte du coût et des technologies de pointe pour leur mise en oeuvre ainsi que de la sensibilité des informations, afin de prévenir la destruction accidentelle et illégale ou la perte accidentelle, l'altération et la communication ou l'accès illicite à leurs fichiers de données à caractère personnel. Pour plus de sécurité, les responsables de traitement sont encouragés à utiliser des mesures spécifiques telles que les technologies de protection de la vie privée (PET = Privacy Enhancing Technologies) et les listes de classement. La convention écrite passée entre le courtier en fichiers et l'utilisateur de la liste doit assurer que les listes sont utilisées conformément aux principes appropriés de sécurité.

3.3.2 Ces mesures comprennent entre autres la sécurité des bâtiments dans lesquels les données à caractère personnel sont conservées (y compris l'accès aux bâtiments), la liste des personnes autorisées (y compris la mention de leurs responsabilités) à accéder aux données, les mécanismes d'authentification appropriés (par ex. contrôle à base de mots de passe) et la sécurité du transfert des données entre les responsables de traitements et le sous-traitant.

³ Voir exemples mentionnés à l'article 2.4.1 plus haut.

⁴ Les listes Robinson sont équivalentes aux Preference Services.

3.3.3 Les responsables de traitements pourront contacter les associations de marketing direct dont ils dépendent pour de plus amples conseils sur les mesures de sécurité appropriées et les technologies de pointe.

3.3.4 Les responsables de traitements devront s'assurer que les sous-traitants auxquels ils font appel disposent de mesures de sécurité appropriées (y compris en matière de confidentialité) en incluant des dispositions à cet effet dans le contrat mentionné à l'article 3.3.1.

3.4 Coordinateur

3.4.1 Les responsables de traitements désigneront un coordinateur chargé de la protection des données au sein de leur organisation afin que celui-ci puisse agir en tant que point de contact pour les questions pertinentes de protection des données.

3.4.2 Les fonctions du coordinateur chargé de la protection des données devront au minimum comprendre :

- le contrôle, seul ou avec une autre personne, de la conformité des pratiques de l'organisation en matière de protection des données par rapport à la législation applicable et aux dispositions de ce code.
- agir en tant qu'interlocuteur auprès des autorités de protection des données compétentes.

3.4.3 Les DMA nationales pourront recueillir les noms des coordinateurs chargés de la protection des données de leurs membres en vue de les transmettre aux autorités de protection des données compétentes.

3.5 Exercice des droits des personnes concernées

Outre le respect des principes décrits au paragraphe 3.1, les responsables de traitements devront se conformer à l'ensemble des droits des personnes concernées tels qu'ils sont définis dans ce code et dans la législation applicable, y compris le droit :

- de refuser que leurs données soient traitées à des fins de marketing direct, y compris le droit de ne pas être contactées pour le compte d'une autre organisation. La conservation des données dans le but de bloquer la communication de marketing direct ne sera pas considérée comme un traitement de marketing direct ;
- de refuser que leurs données soient communiquées à des tiers, sauf dans les cas où une telle communication est exigée par la législation nationale ;
- d'accéder et de rectifier les données qui sont inexactes conformément aux articles 4.1 et 4.2 de ce code ;
- d'exiger l'effacement ou le verrouillage des données quand leur traitement n'est pas conforme aux dispositions de la législation applicable ;
- de s'opposer pour des raisons légitimes et prépondérantes à ce que leurs données soient traitées à d'autres fins que le marketing direct, sauf disposition contraire prévue par la législation applicable.

3.6 Communication de listes

3.6.1 Les responsables de traitements qui communiquent leurs listes à d'autres organisations devront prendre des mesures raisonnables (en demandant par exemple des échantillons de l'offre commerciale) afin d'examiner l'usage que ces organisations prévoient de faire de ces données (par ex. si le contenu du matériel commercial est illégal, contraire à l'éthique ou susceptible de porter atteinte à l'image du marketing direct en général ou si le matériel est de nature inacceptable, telle que la pornographie).

3.6.2 Les responsables de traitements (par exemple les courtiers en fichiers) devront également passer un contrat écrit avec les utilisateurs potentiels (tiers) par lequel ceux-ci s'engagent à respecter les principes de ce code, et ce, avant de communiquer les données.

4 Traitement des demandes émanant des personnes concernées

4.1 Accès aux données

4.1.1 Toute personne concernée a le droit d'obtenir des responsables de traitements :

- La confirmation que ses données personnelles sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées
- La communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données,
- La connaissance de la logique impliquée dans tout traitement automatisé de ses données personnelles, au moins dans le cas des décisions automatisées⁵.

4.1.2 Les responsables de traitements qui reçoivent des demandes, par écrit ou sous toute autre forme durable, émanant de personnes concernées désireuses de connaître les données à caractère personnel les concernant, devront :

- indiquer les informations spécifiques qui pourront être exigées de la part de la personne concernée, notamment en ce qui concerne son identité, afin de s'assurer que la personne concernée est dûment habilitée à exercer son droit d'accès de même que les informations nécessaires à la localisation de données (par ex. la référence de la campagne de publipostage) ;
- communiquer les données à caractère personnel sous une forme intelligible et y joindre toutes les notes ou explications nécessaires pour couvrir les informations ambiguës (par exemple la liste des codes utilisés par les responsables de traitement);
- les informer des coûts raisonnables qu'ils entendent réclamer en échange de la communication des données, de tels coûts ne devant cependant pas dépasser le plafond maximum fixé par la législation nationale ;
- les informer de la logique qui est impliquée dans toute décision individuelle automatisée⁶ de ses données personnelles en vue d'évaluer certains aspects la concernant telle que sa capacité de crédit.

4.1.3 Les responsables de traitements ne sont pas obligés de répondre aux demandes faites à des intervalles déraisonnables (telles qu'elles sont définies par les législations nationales applicables et/ou les codes de déontologie qui prévoient des mesures plus protectrices).

4.2 Rectification

Les responsables de traitements devront répondre à toutes les demandes, par écrit ou sous toute autre forme durable, en vue de rectifier les données à caractère personnel. S'il existe des raisons prépondérantes de douter de la légitimité d'une demande de rectification, des preuves supplémentaires pourraient être exigées avant de procéder à une rectification. Ce sera par exemple le cas quand la demande émane d'une personne mineure sans être approuvée par les parents ou le tuteur ou si les responsables de traitements détiennent des informations démontrant que la demande de rectification des données n'est pas justifiée. Par exemple, si la personne concernée affirme qu'elle n'a jamais commandé de produits auprès d'une société donnée, alors que cette société détient la preuve de cet achat.

⁵ Une décision individuelle automatisée est une décision qui a un effet juridique sur la personne concernée ou qui l'affecte de manière significative et qui est uniquement basée sur un processus automatisé en vue d'évaluer certains aspects de la personne concernée, par exemple en cas de crédit suspect. Une décision individuelle automatisée doit être utilisée conformément à la législation nationale pertinente.

⁶ voir définition dans note 6

Des raisons légitimes et prépondérantes existeront également lorsque les responsables de traitements auront des raisons suffisantes de croire que la demande est excessive. Cela pourra être par exemple dû à la fréquence des demandes.

Si aucune rectification n'est justifiée, la personne concernée devra être informée de cette décision.

4.3 Origine des données

Lorsque les responsables de traitements reçoivent des demandes, par écrit ou sous toute autre forme durable, émanant de personnes concernées, désireuses de connaître l'origine des données les concernant, les responsables de traitements devront, lorsque cela est légal et que l'origine peut être identifiée par le biais d'efforts raisonnables, communiquer ces informations au demandeur. Si les données ont été compilées à partir de différentes origines, les responsables de traitements seront invités à conserver une liste des sources à partir desquelles les données à caractère personnel ont été obtenues.

4.4 Délais de réponse aux demandes de personnes concernées

4.4.1 Les responsables de traitement devront communiquer les informations requises aux articles 4.1, 4.2 et 4.3 dans un délai bref, lequel ne devra pas dépasser les délais autorisés par les dispositions nationales.

4.4.2 La FEDMA recommande que les responsables de traitements communiquent ces informations dans un délai de 20 jours ouvrables, sauf circonstances exceptionnelles.

5 Systèmes de listes d'opposition

5.1 Listes internes d'opposition

- 5.1.1 Les responsables de traitements devront s'assurer que leurs bases de données sont équipées d'un système d'effacement, conçu pour verrouiller les noms (ou tous autres renseignements d'identification pertinents, tels que les numéros de téléphone ou les adresses électroniques, voir note sur les données à caractère personnel dans la section Définitions) des personnes concernées qui ont demandé à ne pas être contactées dans le cadre d'activités de marketing direct.
- 5.1.2 Lorsque les responsables de traitements reçoivent une demande émanant d'une personne concernée demandant à être exclue de toutes leurs activités de marketing direct, ils devront, le plus rapidement possible et dans un délai maximum de 4 semaines après réception de la demande, avoir verrouillé le nom de la personne concernée dans leurs bases de données.
- 5.1.3 Les responsables de traitements qui répondent à la demande de « non-promotion » d'une personne concernée devront expliquer que cet effacement pourra ne pas s'appliquer aux offres de marketing direct qui ont déjà pu être préparées avant réception de la demande. Les responsables de traitement prendront toutes les mesures raisonnables pour s'assurer que la personne concernée ne reçoit plus d'offre de marketing direct le plus rapidement possible et dans un délai maximum de 3 mois après avoir reçu la demande.

5.2 Listes générales d'opposition

- 5.2.1 Les responsables de traitements devront se conformer aux règles des listes nationales d'opposition⁷ lorsque celles-ci existent et, en cas d'utilisation de données à caractère personnel en provenance d'autres pays où de tels services sont en place, devront régulièrement mettre à jour leurs listes par rapport à ces listes d'opposition, conformément aux conventions globales sur les listes d'opposition. Les DMA responsables des listes d'opposition devront également mettre à jour régulièrement leurs fichiers.
- 5.2.2 Les demandes d'effacement seront conservées dans les listes d'opposition pendant une période minimum de trois ans ou plus, selon les règlements nationaux gouvernant les listes d'opposition. Dans le cas particulier des listes d'opposition pour les e-mails, les fichiers doivent être mis à jour dans des délais inférieurs à trois ans, conformément aux règles nationales régissant ces listes d'opposition.
- 5.2.3 Les archives mises à jour des demandes d'effacement devront être conservées pendant une période minimum de trois ans ou plus, selon les règlements nationaux gouvernant les systèmes de listes d'opposition. Dans le cas particulier des demandes de suppression d'e-mails, une période plus brève sera acceptable lorsque les règlements nationaux ou les listes d'opposition pour le e-mail le permettront.

Le propriétaire ou le responsable d'une liste d'opposition devra informer la personne concernée de la durée de validité de sa demande, par exemple quand la personne concernée reçoit la confirmation de sa demande d'effacement.

⁷ Ces listes nationales d'opposition peuvent inclure la liste d'opposition courrier (liste Robinson), la liste d'opposition téléphone, la liste d'opposition fax ou la liste d'opposition e-mail. Il convient de noter cependant que le responsable du traitement devra toujours répondre à l'obligation de recueillir le consentement lorsqu'il utilise des automates d'appel, des facsimiles et des télécopies, conformément à la disposition de la directive 97/66/EC (télécommunication et protection des données), de même que dans le cas d'utilisation des communications électroniques, conformément à la disposition de la directive 2002/58/EC (directive sur la protection des données et les communications électroniques).

6 Transferts de données vers des pays n'appartenant pas à l'Union européenne/l'EEE

En cas de transfert de données vers des pays n'appartenant pas à l'Union européenne/l'EEE et dont on ne considère pas qu'ils disposent d'un niveau de protection adéquat⁸, les responsables de traitements ne pourront transférer des données à caractère personnel que si des garanties suffisantes sont apportées par le biais d'un contrat (lequel devra le plus souvent être approuvé au niveau national) ou en offrant d'autres formes de mécanismes reconnues par l'Union européenne, à moins que la personne concernée n'ait donné clairement son consentement ou que le transfert ne soit nécessaire à l'exécution d'un contrat passé entre la personne concernée et les responsables de traitements ou la mise en oeuvre de mesures précontractuelles adoptées en réponse à la demande de la personne concernée.

⁸ La liste des pays considérés comme offrant une protection adéquate et la procédure prévue par la Commission européenne et les Etats membres devront être utilisées.

7.1 Responsabilité des DMA nationales

Les associations nationales de marketing direct sont responsables de l'application stricte des principes établis dans ce code, tels qu'ils sont incorporés dans les codes nationaux de leurs pays respectifs et devront appliquer les sanctions stipulées dans leurs pays en cas de non-respect de leurs codes nationaux.

Les sociétés devront vérifier régulièrement leur conformité à ce code (par exemple par le biais d'audits internes).⁹

7.2 Résolution des plaintes

7.2.1 Les associations nationales de marketing direct devront établir une procédure en vue de résoudre les plaintes éventuelles pouvant résulter de l'application de ce code au niveau national.

7.2.2 Les associations nationales de marketing direct devront nommer un représentant au sein de chaque association lequel sera chargé de traiter les plaintes et d'agir comme interlocuteur auprès de la FEDMA. Le nom de cette personne devra être communiqué aux autorités de protection des données compétentes

7.2.3 Si une association nationale de marketing direct est dans l'incapacité de résoudre une plainte émanant d'une personne concernée en raison des aspects transfrontaliers de cette demande, celle-ci devra être renvoyée devant la FEDMA, qui nommera alors une personne au sein de la Fédération responsable de la résolution des plaintes.

7.2.4 Les DMA nationales devront coopérer dans la mesure du possible avec les autorités nationales de protection des données dont elles dépendent.

7.2.5 La FEDMA coopérera également avec les autres organisations et organismes gouvernementaux compétents.

7.3 Violation des règles

7.3.1 Toute infraction à ce code par des membres de la FEDMA sera portée devant le comité de protection des données de la FEDMA. Le comité de protection des données, après mûr examen du type d'infraction, pourra décider de recommander auprès du conseil de la FEDMA l'expulsion du membre concerné ou d'autres sanctions à son encontre conformément à ses règles de procédure.

7.3.2 La FEDMA pourra envisager d'intenter des actions à l'encontre d'un membre ou d'un non-membre afin de préserver l'éthique de la profession¹⁰.

7.3.3 Le non-respect des dispositions de ce code pourra également entraîner des actions en justice spécifiques de la part des autorités de contrôle nationales.

7.4 Comité de protection des données

7.4.1 La FEDMA dispose d'un comité de protection de données chargé de contrôler l'application du code FEDMA. Le comité de protection des données dépend du conseil de la FEDMA.

7.4.2 Le comité de protection des données est composé de représentants des DMA nationales définies selon les modalités à l'article 7.2.2, soit un représentant désigné par la FEDMA et trois représentants de sociétés membres du conseil de la FEDMA.

⁹ On tiendra également compte des listes de contrôle élaborées par les autorités de protection des données.

¹⁰ En Belgique par exemple, les organisations professionnelles peuvent engager des actions pour ces motifs.

7.4.3 Les fonctions du comité de protection des données sont les suivantes :

- évaluer annuellement les besoins de révision du code ;
- établir le groupe de travail mentionné à l'article 29 en vue de préparer un rapport annuel sur le code au niveau national et sur les activités transfrontalières ;
- résoudre les plaintes transfrontalières en coopération avec l'IFDMA (la fédération internationale des associations de marketing direct) et l'EASA (l'Alliance européenne en matière de normes publicitaires) ;
- examiner les infractions au code.

7.4.4 Le comité de protection des données devra adopter des règles de procédure internes.