DDMA PRIVACY CODE

Nederlandse Gedragscode

voor het gebruik van

Persoonsgegevens

in het kader van direct marketing

Deze Gedragscode is de vertaling van de
***European Code of Practice for the Use of Personal Data in Direct Marketing*,**
opgesteld door de FEDMA (Federation of European Direct Marketing Associations), waarvan DDMA lid is.

DEFINITIES

DIRECT MARKETING
Communicatie via welk medium dan ook (met inbegrip van, maar niet beperkt tot post, fax, telefoon, on-line diensten, etc.), verricht door de direct marketeer zelf of namens hem, die gericht is aan bepaalde, natuurlijke personen.

PERSOONSGEGEVEN
Een persoonsgegeven[1] is iedere informatie met betrekking tot een geïdentificeerde of identificeerbare natuurlijke persoon. Een identificeerbare persoon is iemand die kan worden geïdentificeerd direct of indirect, in het bijzonder door verwijzing naar een identificatienummer of aan de hand van één of meer factoren die specifiek zijn voor zijn fysieke, fysiologische, mentale, economische, culturele of sociale identiteit.

BIJZONDERE (GEVOELIGE) GEGEVENS
Alle informatie met betrekking tot de volgende gegevens van een persoon wordt gezien als *gevoelige* informatie, en aan verwerking ervan zijn derhalve restricties verbonden:

* Ras of etnische achtergrond.
* Politieke gezindheid.
* Lidmaatschap van een vakvereniging.
* Religieuze of wereldbeschouwelijke overtuiging.
* Psychische of lichamelijke gezondheid.
* Seksuele geaardheid.
* Overtredingen, veroordelingen en beveiligingsmaatregelen.

DIRECT MARKETEER
Elke natuurlijke of rechtspersoon (met inbegrip van charitatieve instellingen en politieke partijen) die via welk medium dan ook (met inbegrip van maar niet uitsluitend per post, fax, telefoon, online-services etc) adverteert, of marketingmateriaal verspreidt dat is gericht aan bepaalde natuurlijke personen.

BETROKKENE
De natuurlijke persoon op wie een persoonsgegeven betrekking heeft.

---

[1] Een persoonsgegeven is iedere informatie met betrekking tot een natuurlijk persoon, die in een zodanige vorm is vastgelegd dat daarmee het individu kan worden geïdentificeerd en die zelfs uit slechts een achternaam kan bestaan. Sommige informatie die geen achternaam bevat moet toch beschouwd worden als een persoonsgegeven en valt daarmee onder deze code. Dit kan bijvoorbeeld het geval zijn met betrekking tot een postadres, telefoonnummer, fax- of e-mailadres, of functieaanduiding indien de persoon op wie dat gegeven betrekking heeft redelijkerwijs kan worden geïdentificeerd door de verantwoordelijke.

COÖRDINATOR GEGEVENSBESCHERMING
Iedere natuurlijke persoon die door de verantwoordelijke is benoemd om de in deze code omschreven functies op zich te nemen.

VERANTWOORDELIJKE
Voor het doel van deze code wordt onder de verantwoordelijke[2] verstaan iedere natuurlijke of rechtspersoon die, alleen of in overleg met andere natuurlijke of rechtspersonen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt en bewaakt.

BEWERKER
Iedere natuurlijke of rechtspersoon, die geen werknemer is van de verantwoordelijke, en die uitsluitend namens de verantwoordelijke en op diens aanwijzing en onder diens verantwoordelijkheid persoonsgegevens verwerkt.

DERDE
Iedere natuurlijke of rechtspersoon die noch de betrokkene is, noch de verantwoordelijke, noch de bewerker[3], noch hun werknemer of vertegenwoordiger.

VERWERKEN
Voor het doel van deze code wordt met verwerken[4] bedoeld: elke geautomatiseerde handeling met betrekking tot persoonsgegevens voor direct marketing-doeleinden. Handmatige handelingen vallen hier ook onder wanneer deze op gestructureerde wijze en aan de hand van specifieke criteria worden uitgevoerd en indien eenvoudige toegang tot de gegevens mogelijk is.

---

[2] De verantwoordelijke moet niet worden verward met de eigenaar van de gegevens. Een bedrijf kan bijvoorbeeld de eigenaar zijn van een database (omdat die natuurlijke of rechtspersoon de materiële rechten bezit voor het gebruik van die database) en kan tegelijkertijd worden aangemerkt als de verantwoordelijke voor de verwerking. De vaardigheden van de verantwoordelijke en de bewerker niet altijd dezelfde. De bewerker is niet noodzakelijkerwijs de berantwoordelijke.

[3] De verantwoordelijke mag bedrijf A als bewerker aanwijzen. De bewerker mag de gegevens alleen volgens de aanwijzingen van de verantwoordelijke verwerken. Indien de verantwoordelijke echter besluit een deel van de gegevens te verhuren aan bedrijf B, dan is dit bedrijf een derde.

[4] De term verwerken heeft betrekking op iedere afzonderlijke schakel van de keten van handelingen met betrekking tot de persoonsgegevens binnen een organisatie: beginnend bij het eerste moment van verzamelen van de gegevens en eindigend bij het vernietigen daarvan, daaronder begrepen iedere andere tussenliggende handeling zoals correctie, onderhoud, opslag en verstrekking aan derden.
Deze code betreft alleen de verwerking van gegevens in relatie tot DM-activiteiten. Marketeers moeten echter nagaan of andere soorten verwerkingen die zij uitvoeren ook in overeenstemming zijn met de toepasselijke regels voor gegevensbescherming.

DERDENVERSTREKKING
Elke vorm van bekendmaken of terbeschikkingstellen van persoonsgegevens (bijvoorbeeld verhuur, verkoop) aan derden.

KINDEREN
Elke natuurlijke persoon jonger dan 14 jaar, tenzij anders gedefinieerd binnen nationale wetgeving of zelfregulering.

OUDER
De ouder(s) of wettelijke vertegenwoordiger van het kind.

1. Toepasselijke recht

1.0. Voor direct marketeers gevestigd binnen het EU/EEA grondgebied
Om vast te stellen aan welke nationale wetten direct marketeers zich moeten houden, moeten ze, indien gevestigd binnen de EU/EEA, de volgende regels in acht nemen:

1.0.0. Wanneer de direct marketeer slechts één vestiging binnen de EU/EEA en derhalve één enkele verantwoordelijke heeft, dan geldt de wet van het land waar de verantwoordelijke is gevestigd, afhankelijk van de regels zoals uiteengezet in punt 1.1.4.

2.0.0. Wanneer de organisatie verscheidene vestigingen in verschillende EU/EEA-lidstaten heeft en wanneer slechts één van die vestigingen als verantwoordelijke kan worden gezien terwijl de andere vestigingen slechts bewerker zijn, moet elke bewerker de nationale wet naleven van de verantwoordelijke, behalve met betrekking tot beveiligingsmaatregelen ten aanzien waarvan de bewerker zijn eigen nationale wet moet naleven.

3.0.0. Wanneer de direct marketeer verscheidene vestigingen in verschillende EU/EEA-lidstaten heeft en elk daarvan afzonderlijk als verantwoordelijke handelt, moet elke vestiging de nationale wet naleven die geldt binnen het land waar de vestiging zetelt.

4.0.0. Wanneer de direct marketeer die optreedt als verantwoordelijke gebruik maakt van een bewerker als vertegenwoordiger die is gevestigd in een ander land binnen de EU/EEA, dan moet de bewerker de wet toepassen die geldt in het land waarin de verantwoordelijke is gevestigd, behalve met betrekking tot beveiligingsmaatregelen waarop de wet van toepassing is, die gelden in het land waar de bewerker is gevestigd.

5.0.0. Het feit dat de gegevens betrekking hebben op natuurlijke personen uit één of meer EU/EEA-landen of uit landen buiten de EU/EEA is niet doorslaggevend bij het vaststellen van de toepasselijke wetgeving.

De verschillende mogelijke situaties zijn om praktische reden samengevat in de volgende matrix:

	Situatie				Toe te passen wet	
Case	**Direct marketeer gevestigd in**	**Verant-woordelijke gevestigd in**	**Bewerker gevestigd in**	**Gegevens uit**	**T.a.v. de verwerking**	**T.a.v. de veiligheids-maatregelen**
1	BE	BE	BE	EU EEA US	BE	BE
2	BE NL UK	BE	NL UK	EU EEA US	BE	NL UK
3	BE	BE NL UK	FR	EU EEA US	BE NL UK	FR
4	BE	BE NL UK	SP PT LUX	EU EEA US	BE NL UK	SP PT LUX

1.0. Voor verantwoordelijken, niet gevestigd binnen de EU/EEA

Wanneer de verantwoordelijke niet gevestigd is binnen de EU/EEA of in een land dat geen adequate bescherming biedt en wanneer de verantwoordelijke geen van de beschermingsmechanismen biedt die door de EU worden ondersteund, moet deze zich aan de nationale wetgeving van een van de lidstaten van de EU/EEA houden wanneer de voor de verwerking gebruikte voorzieningen zich in één van die lidstaten bevindt (bijvoorbeeld een callcenter om de persoonsgegevens te verzamelen, een kantoor dat namens hem persoonsgegevens verwerkt, een listbroker die zijn bestanden bijwerkt, etc.).

1.0.0. De verantwoordelijke moet dan een vertegenwoordiger benoemen (een natuurlijke of rechtspersoon) die gevestigd is in de lidstaat waarin een dergelijke verwerking plaatsvindt. De vertegenwoordiger zal verantwoordelijk zijn voor de contacten met de bevoegde nationale autoriteiten om te garanderen dat de toepasselijke nationale wet door de verantwoordelijke wordt nageleefd. (Dit houdt overigens niet in dat de autoriteiten geen gerechtelijke stappen kunnen ondernemen tegen de verantwoordelijke zelf).

2.0.0. De toepasselijke wet zal de wet zijn van het land waar de vertegenwoordiger is gevestigd.

3.0.0. De bepalingen in artikel 1.2 zijn *niet van toepassing* wanneer de voorzieningen alleen gebruikt worden voor doorvoerdoeleinden binnen de EU/EEA (bijvoorbeeld wanneer de verantwoordelijke gevestigd is in Canada, de gegevens verzameld zijn in landen buiten de EU/EEA en deze via een telecommunicatiediensten-aanbieder in de UK naar Canada worden verzonden).

2. Het verzamelen van persoonlijke gegevens

1.0. Verzamelen rechtstreeks bij de betrokkene

De verantwoordelijke moet er op toezien dat de gegevens op een eerlijke manier worden verzameld en dat het recht op informatie van de betrokkene, zoals beschreven in deze code, wordt verzekerd.

Algemene regels voor eerlijke verwerking

* *Essentiële informatie*
  De verantwoordelijken moeten ervoor zorgdragen dat de betrokkenen worden geïnformeerd over:

  * De identiteit van de verantwoordelijke (bijvoorbeeld naam en adres).
  * Het doel van de verwerking (bijvoorbeeld contractuele - of reclamedoeleinden).

  De essentiële informatie moet ten tijde van het verzamelen van de gegevens worden verstrekt, tenzij deze onomstotelijk blijkt uit de context (bijvoorbeeld wat de identiteit van de verantwoordelijke en het doel betreft, indien de naam van het bedrijf duidelijk wordt vermeld in de reclame) of wanneer de betrokkene al over de informatie beschikt (bijvoorbeeld wanneer deze een overeenkomst is aangegaan met het bedrijf).

* *Informatie over de rechten op inzage, correctie van gegevens en bezwaar*
  De verantwoordelijken moeten ervoor zorgdragen dat de betrokkenen geïnformeerd worden over:

  * Het recht op inzage en het recht om onjuiste gegevens te (laten) corrigeren die op hun betrekking hebben.
  * Het recht om niet te worden benaderd voor DM-doeleinden.
  * Het recht om bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens voor DM-doeleinden.

Omgaan met specifieke situaties

* *Informatie bij gebruik gegevens voor DM-activiteiten van de verantwoordelijke*
  Wanneer het de bedoeling is dat de verantwoordelijke de gegevens voor eigen DM-doeleinden gebruikt, moet deze ervoor zorg dragen dat de betrokkene zich bewust is van de essentiële informatie en van zijn of haar recht om verschoond te blijven van dit gebruik. De verantwoordelijke moet de infor-

matie verschaffen ten tijde van het verzamelen van de gegevens en moet alles in het werk stellen om dit daadwerkelijk te doen. Maar in het geval dat dit moeilijk of onmogelijk is (bijvoorbeeld bij kleine rubrieksadvertenties of telemarketing) en wanneer dit binnen de nationale wetgeving is toegestaan, mag deze informatie ook zo snel mogelijk na het verzamelen worden verstrekt, bijvoorbeeld wanneer de betrokkene de eerste documentatie - hetzij schriftelijk, hetzij via een ander duurzaam medium (bijvoorbeeld rekening, ontvangstbevestiging etc.) - ontvangt.

* *Informatie in geval van derdenverstrekking*
  Wanneer het de bedoeling is om de gegevens ook aan derden te verstrekken moet de verantwoordelijke ervoor zorgen dat de betrokkene, naast de genoemde essentiële informatie, ook wordt geïnformeerd over:

  * Enige ontvanger of categorie van ontvangers van de gegevens en het doel waarvoor die gegevens worden verstrekt.
  * Zijn of haar recht om niet mee te werken aan verstrekking voor DM-doeleinden.

  Deze informatie moet worden gegeven ten tijde van het verzamelen en alles moet in het werk worden gesteld om dit te doen, maar waar dit moeilijk of onmogelijk mocht zijn (bijvoorbeeld bij kleine rubrieksadvertenties of telemarketing) en wanneer dit binnen het kader van de Wet Bescherming Persoonsgegevens is toegestaan, moet deze informatie worden verstrekt voordat er enige bekendmaking aan derden plaatsvindt.

  Het kan zijn dat deze informatie niet hoeft te worden verstrekt wanneer dit al is gebeurd via daartoe geëigende mechanismen (bijvoorbeeld via een geschikte gezamenlijke kennisgeving die algemeen toegankelijk is en voldoende gericht op een specifiek publiek). Deze mechanismen moeten binnen het kader van de nationale wetgeving zijn toegestaan en moeten kenbaar zijn gemaakt in overeenstemming met de wettelijke vereisten van de toepasselijke nationale wetgeving.

* *Informatie in geval van gebruik van vragenlijsten en dergelijke*
  In aanvulling op de genoemde essentiële informatie dienen verantwoordelijken ervoor te zorgen dat zij de betrokkenen laten weten of het beantwoorden van de vragen verplicht is dan wel op vrijwillige basis plaatsvindt, en wat de mogelijke consequenties zijn van het niet invullen van de vragen (bijvoorbeeld - inclusief maar niet daartoe beperkt tot - het niet ontvangen van een geschenk bij het verzamelen van gegevens aan de

hand van vragenlijsten). De verantwoordelijke moet er ook voor zorg-dragen dat er geen onnodige vragen worden gesteld.

Bij het verzamelen van gegevens aan de hand van vragenlijsten moet die informatie worden gegeven ten tijde van het verzamelen van de gegevens.

2.0. Verzamelen via andere bronnen dan de betrokkene

1.0.0 Wanneer een verantwoordelijke de persoonsgegevens niet bij de betrokkene zelf verzamelt, is hij verplicht die stappen te ondernemen die noodzakelijk zijn om ervoor te zorgen dat de betrokkene niettemin op de hoogte is van de informatie die hij of zij zou hebben ontvangen wanneer er wel rechtstreeks contact met de verantwoordelijke had plaatsgevonden. Bijvoorbeeld bij gehuurde bestanden of zogenoemde "member get member"-campagnes, òf bij het verzamelen van gegevens aan de hand van vragenlijsten, moet in het bijzonder voldaan worden aan de legitimiteitprincipes, zoals gedefinieerd in artikel 2.1.

2.0.0 De verantwoordelijke moet de informatie, zoals beschreven in artikel 2.1, verstrekken:

* Op het moment van vastlegging (d.w.z. verwerking) van de gegevens.
* Of, wanneer bekendmaking aan een derde wordt voorzien, niet later dan op het moment van bekendmaking, tenzij de betrokkene reeds is geïnformeerd.

1.0.0. In afwijking op de in artikel 2.2.1 genoemde bepalingen en vooropgesteld dat de gebruikte gegevens aanvankelijk zijn verzameld met inachtneming van de regels op het gebied van gegevensbescherming, zijn de hierboven genoemde eisen niet van toepassing in specifieke buitengewone omstandigheden waarin een onevenredig grote inspanning moet worden geleverd om dergelijke informatie te verstrekken en waar is voorzien in aanvullende geëigende waarborgen, zoals vastgelegd in nationale wetgeving. In het bijzonder in die omstandigheden waarin sprake is van onevenredig hoge kosten in termen van tijd of geld. Bijvoorbeeld wanneer gegevens worden verkregen van een derde en wanneer deze spoedig daarna zullen worden gebruikt, zou het onevenredig zijn om de betrokkene meteen te moeten informeren, wanneer dit ook kan wachten tot het eerste contact met de betrokkene zelf plaatsvindt.

2.0.0. Deze factoren moeten steeds goed worden afgewogen tegen de gevolgen voor de betrokkenen bij gebruikmaking van de afwijking. Omstandigheden waaronder afwijking op grond van onevenredige inspanning van toepassing zou kunnen zijn, terwijl alle overige omstandigheden gelijk blijven, zijn:

* Persoonsgegevens die worden bewaard met als doel blokkering of verificatie van adresgegevens.
* Bij suppressie van persoonsgegevens als gevolg van de toepassing van een Robinson List of een Preference Service-bestand.
* Bij verwijdering of suppressie door de marketeer van de persoonsgegevens van diegenen in het marketingbestand die niet overeenkomen met het vereiste profiel.

3.0.0. Wanneer de verantwoordelijke, na afweging van de relevante factoren, heeft besloten om gebruik te maken van de afwijking, dan moet hij waarborgen dat er een schriftelijke verklaring (waarin de onderliggende reden van de beslissing, een omschrijving van de informatie die de verantwoordleijke gegeven zou hebben, een verklaring waarom de betrokkene niet wordt geschaad door de toepassing van de afwijking) is voorbereid, en dat deze vervolgens beschikbaar is ter rechtvaardiging van de beslissing.

3.0. Het verzamelen van bijzondere (gevoelige) gegevens)

Vanwege het bijzondere belang van bijzondere gegevens met betrekking tot de fundamentele privacy-rechten van de betrokkene, moet er bijzondere zorg worden betracht bij het verwerken van dergelijke gegevens.

Wanneer bij de persoonsgegevens die worden verzameld bijzondere gegevens betrokken zijn, moet de verantwoordelijke uitdrukkelijke toestemming van de betrokkene vragen om die persoonsgegevens te mogen verzamelen en verder te verwerken. Uitdrukkelijke toestemming betekent dat de betrokkene deze vrijwillig en specifiek en op grond van voldoende informatie heeft gegeven op een zodanige wijze dat er geen verdere actie nodig is om vast te stellen waarvoor hij of zij de toestemming heeft verleend. Uitdrukkelijke toestemming hoeft niet per definitie schriftelijk te worden gegeven, maar in de praktijk gebeurt dat vaak wel omdat dit een goed middel is voor bewijs van de toestemming, tenzij:

* De gegevens duidelijk door de betrokkene zelf openbaar zijn gemaakt (bijvoorbeeld via een voor ieder toegankelijke bron zoals een (telefoon)gids, ten aanzien waarvan de betrokkene de mogelijkheid heeft gehad zijn gegevens daarin niet te laten opnemen).
* Of wanneer de informatie wordt verwerkt door een relevante non–profit-organisatie met een doelstelling op politiek, filosofisch, religieus of vakbondsgebied. Wanneer deze instanties de gegevens verwerken zonder uitdrukkelijke toestemming van de betrokkene, moeten zij er rekening mee houden dat:

* De verwerking moet worden uitgevoerd binnen de legitieme activiteiten van deze instanties.
* Er gepaste waarborgen moeten worden geboden.
* De verwerking alleen betrekking mag hebben op leden van de instantie of personen waarmee de instantie regelmatig contact onderhoudt.
* De verwerking moet plaatsvinden in relatie tot de doelen van de non profit-organisatie.
* De informatie niet verstrekt wordt aan een derde zonder toestemming van de betrokkene.

Een voorbeeld van dit soort activiteiten zou een kerkelijk genootschap kunnen zijn dat, ofwel via een bewerker ofwel zelf, brieven naar haar leden stuurt waarin zij de publicatie van een religieus bulletin aankondigt waarop geïnteresseerden zich kunnen abonneren, of waarmee zij fondsen werft om in een bijzondere situatie hulp en bijstand te bieden.

Bedrijven mogen onder geen enkele omstandigheid bijzondere gegevens gebruiken op een zodanige wijze dat de fundamentele rechten en vrijheden van de betrokkene geschaad kunnen worden. Gegevens moeten te allen tijde voor legitieme activiteiten worden verwerkt.

Wanneer bijzondere gegevens, die verzameld zijn in verband met DM-activiteiten, verder worden verwerkt voor statistische analyse-doeleinden, moeten deze worden geanonimiseerd of tenminste zo gewijzigd dat identificatie van de betrokkenen niet mogelijk gemaakt wordt, tenzij de verantwoordelijke daarvoor uitdrukkelijktoestemming heeft verkregen.

1.0 Verschillende doeleinden

1.0.0 Wanneer men de gegevens wil gaan verwerken voor een ander doel dan waarvoor de gegevens oorspronkelijk zijn verzameld, moet de verantwoordelijke nagaan of het nieuwe doel verenigbaar is met het aangegeven doel. Wanneer het verenigbaar is, is verwerking voor dit nieuwe doel toegestaan. Wanneer het nieuwe doel niet verenigbaar is met de aangegeven doelstelling, is verdere verwerking alleen toegestaan wanneer dit in overeenstemming is met de toepasselijke wetgeving met betrekking tot gegevensbescherming.

2.0.0 Bij het beoordelen van de verenigbaarheid van het nieuwe doel, moeten de verantwoordelijken onder andere rekening houden met de volgende criteria:

* Of het nieuwe doel wezenlijk anders is dan het doel waarvoor de gegevens zijn verzameld.
* Of de betrokkenen redelijkerwijs hadden kunnen voorzien of dat het waarschijnlijk is dat zij bezwaar hadden gemaakt als zij het hadden geweten.

De verantwoordelijke moet altijd rekening houden met relevante nationale richtlijnen uitgevaardigd door de relevante autoriteit met betrekking tot de bescherming van persoonsgegevens.

2.0 Host-mailings

1.0.0 Van host-mailings is sprake wanneer een verantwoordelijke materiaal van een derde opneemt in zijn eigen mailing.

2.0.0 Bij een host-mailing moet de verantwoordelijke duidelijk te identificeren zijn. Selectiecriteria die een nadelig effect zou hebben op de rechten van de betrokkene - bijvoorbeeld het gebruik van bijzondere gegevens gekoppeld aan een aankooppatroon (verrichte aankopen van een farmaceutisch product) mogen niet gebruikt worden.

3.0 Speciale bepalingen met betrekking tot kinderen

1.0.0 Bij het verzamelen van gegevens over kinderen moeten verantwoordelijken altijd al het mogelijke doen om te waarborgen dat het kind en/of zijn ouder naar behoren zijn geïnformeerd over de doeleinden waarvoor de gegevens van het kind worden verwerkt.

2.0.0 Vooral wanneer gebruikt wordt gemaakt van commercieel en op het kind gericht materiaal of wanneer op een andere manier bewust gegevens van kinderen worden verzameld, moet deze informatie duidelijk, gemakkelijk toegankelijk en begrijpelijk voor kinderen zijn.

3.0.0 Daar waar toepasselijke nationale of Europese wetgeving op het gebied van gegevensbescherming voorschrijft dat de betrokkene toestemming moet geven voor verwerking van gegevens, moet de verantwoordelijke geïnformeerde en voorafgaande toestemming van de ouder verkrijgen. De manier waarop dit moet gebeuren, moet altijd in overeenstemming zijn met de toepasselijke wetgeving en zelfregulering.

4.0.0 De verantwoordelijke moet de ouder van het kind dezelfde rechten over de gegevens van het kind geven als omschreven in artikel 3.5 van deze code. De verantwoordelijke moet elke redelijke inspanning doen om te verifiëren dat degene die de rechten van het kind uitoefent de ouder is.

5.0.0 De verantwoordelijke mag bij het aanbieden van een prijs of bij enige andere activiteit met een verkoopbevorderend voordeel voor deelname van het kind aan een spel niet als voorwaarde stellen, dat het kind meer persoonsgegevens bekend maakt dan strikt noodzakelijk zijn voor de deelname aan een dergelijke activiteit.

2 Verplichtingen van de verantwoordelijke

1.0 Beginselen van gegevensbescherming

1.0.0 De verantwoordelijke moet handelen overeenkomstig de volgende beginselen. Persoonsgegevens moeten:

* Op een behoorlijke en gerechtvaardigde wijze verwerkt worden op basis van een legitieme reden, in overeenstemming met de toepasselijke wet en met de bepalingen in deze Code.
* Worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigd doeleinden (bijvoorbeeld de bij het College Bescherming Persoonsgegevens gemelde doeleinden zoals handel in persoonsinformatie, koop op afstand-activiteiten).
* Niet verder worden verwerkt op een manier die onverenigbaar is met deze doeleinden (zie de voorbeelden genoemd in art. 2.4.1) tenzij de betrokkene daarvoor zijn of haar toestemming heeft gegeven.
* Toereikend, terzake dienend (het is bijvoorbeeld gewoon dat een luchtvaartmaatschappij haar passagiers naar hun eetgewoonten vraagt teneinde de juiste maaltijd te kunnen geven, terwijl het normaal gesproken niet gebruikelijk is dat een autobedrijf naar de eetgewoonten van haar klanten informeert omdat deze haar klanten normaliter geen maaltijden serveert), en niet bovenmatig ten opzichte van het doel waarvoor zij worden verzameld en/of verder worden verwerkt.
* Juist en bijgewerkt zijn. Dit kan worden gerealiseerd door gebruik te maken van suppressielijsten (zowel interne als het zogenoemde. Infofilter), aan de hand van publiekelijk beschikbare gegevens en doordat betrokkenen gebruik maken van hun correctierecht.
* Niet langer in een vorm worden bewaard die het mogelijk maakt de betrokkene te identificeren dan noodzakelijk is voor de doeleinden waarvoor de gegevens worden verzameld en vervolgens worden verwerkt.

2.0.0 De verantwoordelijken moeten een overeenkomst met hun bewerkers aangaan, waarin de bewerker akkoord gaat met met het nakomen van deze beginselen en er tevens mee akkoord gaat alleen op instructie van de verantwoordelijke te zullen handelen. De verantwoordelijkheid voor een behoorlijke en gerechtvaardigde wijze van verwerking blijft op de verantwoordleijke rusten en kan niet door middel vaneen contract worden overgrdragen aan een bewerker.

1.0. Melding bij de Autoriteit met betrekking tot Bescherming Persoonsgegevens

De verantwoordelijken dienen ervoor te zorgen dat hun gegevensverwerking worden gemeld overeenkomstig de. relevante toepasselijke wetgeving.

2.0. Beveiligingsmaatregelen

1.0.0. De verantwoordelijke dient ervoor te zorgen dat hij, rekening houdend met de kosten, de beschikbare technologie en met de gevoeligheid van de gegevens, alle passende beveiligingsmaatregelen treft om te voorkomen dat ongewilde en onwettige vernietiging of verlies, wijziging of niet toegestane derdenverstrekking of toegang tot de bestanden met persoonsgegevens plaatsvindt.
Als extra waarborg wordt verantwoordelijken aanbevolen om speciale maatregelen te treffen, zoals Privacy Enhancing Technologies (de zogenoemde PET´s) en 'seeding lists'. De schriftelijke afspraak tussen de listbroker en de bestandsgebruiker moet waarborgen dat de bestanden worden gebruikt met inachtneming van geëigende beveiligingsbeginselen.

2.0.0. Bovengenoemde maatregelen bevatten o.a. beveiliging van de gebouwen waar de persoonsgegevens worden opgeslagen en/of verwerkt (inclusief de toegang tot het gebouw), een lijst met personen die geautoriseerd zijn om toegang te hebben tot de gegevens (met vermelding van hun aansprakelijkheid), geschikte echtheidscontrole-mechanismen (bijvoorbeeld wachtwoordcontrole) en beveiliging bij doorgifte van gegevens tussen de verantwoordelijke en de bewerker.

3.0.0. De verantwoordelijke kan verwijzen naar de DDMA en andere relevante (branche)organisaties waar het voorlichting betreft over beveiligingsmaatregelen en beschikbare technologie.

4.0.0. De verantwoordelijke moet zich ervan overtuigen dat elke bewerker van wiens diensten hij gebruik maakt gepaste beveiligingsmaatregelen toepast, ook met

betrekking tot vertrouwelijkheid, door hierover bepalingen op te nemen in de in artikel 3.3.1 vermelde overeenkomst.

2.0. Aanspreekpunt

1.0.0. De verantwoordelijke moet een coördinator voor de gegevensbescherming aanstellen binnen de organisatie, die fungeert als aanspreekpunt voor relevante kwesties op het gebied van gegevensbescherming.

2.0.0. De taken van de coördinator voor de gegevensbescherming moeten in ieder geval omvatten:

* Het alleen of met iemand anders bewaken dat de organisatie bij haar activiteiten op het gebied van gegevensbescherming de van toepassing zijnde wet en de bepalingen in deze Code naleeft;
* Als aanspreekpunt dienen voor de relevante autoriteiten met betrekking tot de bescherming persoonsgegevens.

3.0.0. De nationale DMA's mogen de namen van de coördinatoren van de gegevens-bescherming van hun leden verzamelen teneinde deze door te geven aan de relevante autoriteit met betrekking tot de bescherming van persoonsgegevens.

3.0. Uitoefening van de rechten van de betrokkene

Naast het zich houden aan de bepalingen zoals omschreven onder 3.1, moet de verantwoordelijke ook handelen overeenkomstig de rechten van de betrokkenen - zoals omschreven in deze Code en in de toepasselijke wetgeving, met inbegrip van:

* Het recht om bezwaar te maken tegen de verwerking van zijn gegevens voor DM-doeleinden daaronder begrepen de mogelijkheid om niet namens een ander te worden benaderd.
* Het vasthouden van gegevens met als doel het blokkeren van communicatie voor DM-doeleinden wordt niet beschouwd als een verwerking voor DM-doeleinden.
* Het recht om bezwaar te maken tegen verstrekken van gegevens aan een derde, behalve daar waar een dergelijke verstrekking wordt vereist door nationale wetgeving.
* Het recht op inzage van de gegevens en correctie van onjuiste gegevens overeenkomstig de artikelen 4.1 en 4.2 van deze Code.

* Het recht tot het eisen van verwijdering of blokkering van gegevens wanneer verwerking daarvan niet plaatsvindt overeenkomstig de bepalingen van de toepasselijke wetgeving.
* Het recht om op legitieme dringende gronden bezwaar te maken tegen de verwerking van gegevens voor andere dan DM-doeleinden, tenzij anders bepaald binnen de geldende wetgeving.

1.0. Derdenverstrekking van bestanden

1.0.0. Verantwoordelijken die hun bestanden verstrekken aan andere organisaties, moeten redelijke stappen ondernemen (bijvoorbeeld een voorbeeld van het gebruikte materiaal opvragen) om de bedoelingen achter het gebruik van de gegevens door die organisaties te onderzoeken (bijvoorbeeld is de inhoud van het materiaal mogelijk illegaal, onethisch, of brengt het waarschijnlijk schade toe aan het imago van Direct Marketing in het algemeen, of bevat het materiaal dat onaanvaardbaar is, zoals bijvoorbeeld pornografie?).

2.0.0. Verantwoordelijken (bijvoorbeeld listbrokers) moeten, vóór het verstrekken van de gegevens, ook een schriftelijke overeenkomst sluiten met de beoogde gebruiker (de derde) waarin deze verklaart zich te zullen houden aan de beginselen uit deze Code.

1. Behandeling van verzoeken van betrokkenen

1.0. Inzagerecht

1.0.0. Iedere betrokkene heeft het recht om van de verantwoordelijke:

* Een bevestiging te ontvangen over het feit of al dan gegevens hem/haar betreffende worden verwerkt en informatie tenminste over de doeleinden van de verwerking, over de categorieën van de desbetreffende gegevens en over de ontvangers of categorieën en ontvangers aan wie de gegevens worden verstrekt.
* In een begrijpelijke vorm informatie te ontvangen over de gegevens die worden verwerkt en beschikbare informatie over de bron van die gegevens.
* Informatie te ontvangen over de logica die ten grondslag ligt aan een geautomatiseerde verwerking in geval van geautomatiseerde besluiten.

2.0.0. Verantwoordelijken die – schriftelijk of via een ander duurzaam medium – verzoeken van een betrokkene ontvangen om gegevens over hunzelf in te zien, moeten:

* Aangeven welke speciale informatie over de betrokkene nodig mocht zijn, in het bijzonder over diens identiteit, om zowel zeker te kunnen stellen dat de betrokkene werkelijk recht heeft op inzage als om zijn/haar gegevens te kunnen lokaliseren (bijvoorbeeld referenties met betrekking tot mailing-campagnes).
* De persoonsgegevens in een pasklare begrijpelijke vorm aanleveren en notities of verklaringen met betrekking tot een mogelijke dubbelzinnige uitleg van de informatie toevoegen, bijvoorbeeld een lijst met de door de verantwoordelijke gebruikte codes.
* Informeren over enige redelijke- vergoeding die zij zullen vragen voor het verstrekken van de gegevens; indien toegestaan bij nationale wet, mag een dergelijke vergoeding niet hoger zijn dan is toegestaan op grond van nationale regelgeving.
* De betrokkene informeren over de logica bij geautomatiseerde verwerking van diens gegevens met als doel zaken te beoordelen die hem/haar betreffen, bijvoorbeeld i.v.m. kredietwaardigheid van de betrokkene.

3.0.0. Verantwoordelijken zijn niet verplicht om vragen te beantwoorden die met onredelijke tussenpozen worden gesteld (zoals gedefinieerd in nationale toepasselijke wetten en/of gedragsregels die verdere beschermende maatregelen bieden).

1.0. Correctie

De verantwoordelijke moet actie ondernemen naar aanleiding van ieder verzoek,schriftelijk of via een ander duurzaam medium, om persoonsgegevens te corrigeren. Wanneer er dringende gronden zijn om te twijfelen aan de legitimiteit van een verzoek tot correctie, moet verder bewijs worden opgevraagd voordat de correctie wordt uitgevoerd. Dit kan bijvoorbeeld het geval zijn bij een verzoek door een minderjarige zonder toestemming van de ouder(s) of voogd, of wanneer de verantwoordelijke over informatie beschikt die aantoont dat het verzoek om de gegevens aan te vullen niet gerechtvaardigd is. Bijvoorbeeld wanneer de betrokkene zegt nooit iets bij een bedrijf te hebben besteld terwijl het bedrijf kan aantonen dat dit wel het geval is.

Dringende gewettigde gronden zijn eveneens aanwezig wanneer er voldoende aanleiding bestaat om aan te nemen dat het verzoek bovenmatig is. Dit kan bijvoorbeeld het gevolg zijn van de veelvuldigheid van het verzoek.

Wanneer een wijziging niet gerechtvaardigd is, wordt de betrokkene op de hoogte gesteld van deze beslissing.

1.0 Bron van de gegevens

Wanneer de verantwoordelijke een verzoek van een betrokkene ontvangt - schriftelijk of via een ander duurzaam medium - waarin gevraagd wordt naar de bron van de gegevens, moet de verantwoordelijke, wanneer dit wettelijk is toegestaan en wanneer het mogelijk is om met een redelijke inspanning de bron te achterhalen, de informatie aan de verzoeker verstrekken. Wanneer gegevens zijn samengesteld uit verscheidene bronnen, is het aan te bevelen dat verantwoordelijken een lijst bijhouden van de bronnen waaruit de persoonsgegevens zijn verkregen.

1.0. Termijn voor afhandeling van verzoeken van betrokkenen

1.0.0. De verantwoordelijke moet de informatie zoals omschreven in art. 4.1, 4.2 en 4.3 binnen een korte termijn verstrekken, deze termijn mag in ieder geval niet langer zijn dan de termijn die in de toepasselijke nationale regels is toegestaan.

2.0.0. FEDMA adviseert dat verantwoordelijken dergelijke informatie binnen 20 werkdagen verstrekken, tenzij er zich buitengewone omstandigheden voordoen.

2. "Preference Services"-systemen

1.0. Interne suppressielijsten (blokkeringsbestanden)

1.0.0. De verantwoordelijke moet waarborgen dat er binnen zijn database een blokkeringssysteem geactiveerd is, nodig om namen (en andere relevante details over identiteit, zoals telefoonnummers of email-adressen [zie noot met betrekking tot persoonsgegevens in het hoofdstuk "Definities"]) van betrokkenen die hebben aangegeven niet te willen worden benaderd voor DM-doeleinden, te blokkeren.

2.0.0. Wanneer de verantwoordelijke een verzoek ontvangt om de betrokkene op geen enkele manier te benaderen, moet hij zo spoedig mogelijk en ten minste binnen 4 weken na ontvangst van het verzoek, de naam van die betrokkene hebben geblokkeerd in zijn database.

3.0.0. De verantwoordelijke moet de betrokkene die een zogenoemde. "geen reclame"-verzoek heeft ingediend, laten weten dat blokkering niet van toepassing is op DM-materiaal dat al was voorbereid voordat het verzoek werd ontvangen. De verantwoordelijke moet al het mogelijke in het werk stellen om te waarborgen dat de betrokkene, zodra deze een verzoek heeft ingediend, zo spoedig mogelijk geen verder DM-materiaal zal ontvangen, en tenminste met ingang van uiterlijk 3 maanden na ontvangst van het verzoek.

2.0. "Preference Service"-systemen

1.0.0. De verantwoordelijke dient de beginselen.van de nationale Preference Services in het land waar hij zijn activiteiten ontploooit na te leven, en indien de verantwoordelijke persoonsgegevens gebruikt uit andere landen waarin dergelijke Preference Services worden gehanteerd, dient hij regelmatig zijn bestanden op te schonen aan de hand van die Preference Services, een en ander overeenkomstig de *Global Conventions on Preference Services*. De DMA's die een preference service onder zich hebben, dienen hun bestanden regelmatig op te schonen.

2.0.0. Verzoeken tot blokkering moeten binnen de preference service-systemen tenminste 3 jaar bewaard worden, of zoveel langer als bepaald binnen de nationale regelgeving op het gebied van preference services. In het bijzonder geval van email preference-services kan het zijn dat bestanden binnen een kortere termijn dan 3 jaar moeten worden bijgewerkt, een en ander overeenkomstig de nationale regelgeving ten aanzien van e-MPS.

Een actueel bijgewerkt archief van de verzoeken tot blokkering moet minimaal 3 jaar worden bewaard, of zoveel langer als vastgelegd binnen de nationale regelgeving of de nationale preference service. In het specifieke geval van verzoeken tot blokkering voor e-mail is een kortere termijn acceptabel daar waar de nationale regelgeving of de "Preference Service" dit toestaat.

3.0.0. De eigenaar of beheerder van het "Preference Service"-systeem moet de betrokkene informeren over de termijn gedurende welke het verzoek geldig blijft. Dit kan bijvoorbeeld gebeuren bij bevestiging van ontvangst van het verzoek van blokkering aan de betrokkene.

2. Doorgiften van gegevens naar landen buiten de EU 6

Bij overdracht van gegevens naar landen buiten de EU/EEA, waarvan wordt aangenomen dat ze niet over een adequaat beschermingsniveau beschikken[5], kan de verantwoordelijke alleen persoonsgegevens overdragen wanneer in voldoende waarborgen is voorzien, zoals door het opstellen van een overeenkomst (vaak moet dit op nationaal niveau worden goedgekeurd) of aan de hand van een andere door de EU goedgekeurd mechanisme, tenzij de betrokkene zijn of haar onbetwistbare toestemming heeft gegeven of tenzij de doorgifte noodzakelijk is voor de uitvoering van een overeenkomst tussen de betrokkenen en de verantwoordelijke, of noodzakelijk is voor de implementatie van precontractuele maatregelen die genomen worden naar aanleiding van het verzoek van de betrokkene.

1. Naleving en toezicht

1.0. Verantwoordelijkheden van de nationale DMA's

De nationale DMA's zijn verantwoordelijk voor de strikte toepassing van de beginselen zoals omschreven in deze Code, zoals opgenomen in hun nationale codes in hun respectievelijke landen en moeten dezelfde sancties toepassen als voorgeschreven zijn voor de niet-naleving van hun nationale codes.
Bedrijven moeten regelmatig de naleving van deze code controleren (bijvoorbeeld door middel van self-audits.

1.0. Klachtenbehandeling

1.0.0. De nationale DMA's moeten een procedure vaststellen voor het behandelen van klachten die kunnen voortvloeien uit het toepassen van deze Code op nationaal niveau.

2.0.0. De nationale DMA's wijzen binnen de vereniging een persoon aan die verantwoordelijk is voor het afhandelen van de klachten en die in dezen als contactpersoon voor FEDMA fungeert. De naam van deze persoon wordt bekendgemaakt aan de desbetreffende autoriteit met betrekking tot de bescherming van persoonsgegevens.

5. De lijst van landen waarvan wordt verondersteld dat zij niet over een gepast niveau van bescherming beschikken en de procedure zoals verstrekt door de Europese Commissie en de nationale lidstaten moeten hier worden gebruikt.

3.0.0. Wanneer de nationale DMA, in verband met grensoverschrijdende aspecten, niet in staat is een klacht van een betrokkene op te lossen, moet deze de kwestie voorleggen aan de FEDMA, die iemand binnen de Federatie zal benoemen die verantwoordelijk is voor de behandeling van klachten.

4.0.0. De nationale DMA's moeten zoveel mogelijk samenwerken met hun nationale autoriteiten met betrekking tot de bescherming van persoonsgegevens.

5.0.0. FEDMA zal ook samenwerken met andere relevante organisaties en overheids-instanties.

2.0. Overtreding van de beginselen

1.0.0. Iedere overtreding van deze Code door leden van de FEDMA zal ter beoordeling worden voorgelegd aan het *FEDMA Data Protection Committee*. Het Data Protection Committee kan, rekening houdend met het soort overtreding, besluiten om de FEDMA Board te adviseren om het lid ofwel te royeren ofwel een andere sanctie op te leggen, overeenkomstig haar procedureleregels.

2.0.0. FEDMA kan overwegen om tegen een lid of niet-lid een actie te starten teneinde de beroepsethiek te waarborgen.[6]

3.0.0. Het niet naleven van de bepalingen in deze Code kan eveneens resulteren in specifieke juridische acties vanuit de nationale autoriteiten met betrekking tot de bescherming van persoonsgegevens.

3.0. Data Protection Committee

1.0.0. Binnen de FEDMA wordt een Data Protection Committee opgericht dat de toepassing van de FEDMA Code controleert. Het Data Protection Committee rapporteert aan de FEDMA Board.

2.0.0. Het Data Protection Committee bestaat uit de contactpersonen van de nationale DMA´s, zoals vastgesteld in art. 7.2.2, de benoemde contactpersoon binnen FEDMA en 3 vertegenwoordigers van bedrijven die lid moeten zijn van de FEDMA Board.

---

6. In België bijvoorbeeld kunnen beroepsorganisaties op deze gronden acties ondernemen.

3.0.0. De taken van het Data Protection Committee zijn:

* Jaarlijks overwegen of een aanpassing van de Code noodzakelijk is.
* Het aan de Art.29 Werkgroep aanbieden van een jaarverslag met betrekking tot het functioneren van de code op nationaal niveau en bij grens-overschrijdende activiteiten.
* Het oplossen van grensoverschrijdende klachten in samenwerking met de IFDMA (International Federation of Direct Marketing Associations) en de EASA (European Advertising Standards Alliance).
* Het in overweging nemen van welke overtreding dan ook van de Code.

1.0.0. Het Data Protection Committee moet interne procedurele regels vaststellen.