

**CODICE DI
AUTODISCIPLINA,
DI DEONTOLOGIA
E DI BUONA CONDOTTA
RISPETTO AI TRATTAMENTI
DI DATI PERSONALI
EFFETTUATI PER FINALITÀ
DI MARKETING DIRETTO,
DI VENDITA A DISTANZA E DI
VENDITA DIRETTA**

Preambolo

Il presente codice è volto a garantire che l'utilizzazione di dati di carattere personale per scopi di direct marketing, di vendita a distanza, di vendita diretta oltre che di comunicazione commerciale diretta o interattiva, si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, in particolare del diritto alla riservatezza e del diritto all'identità personale.

Il codice è espressione dell'autonomia degli operatori professionali che intendono utilizzare dati personali per comunicare con clienti, potenziali clienti e categorie di consumatori individuati secondo criteri predeterminati mediante messaggi diretti.

Il presente codice esprime l'applicazione, a livello nazionale, delle regole definite dal Codice europeo di buona condotta in materia di direct marketing approvato dalla FEDMA nel maggio 2003 (che il 13 giugno 2003 il Gruppo di lavoro per la tutela dei dati personali istituito ai sensi dell'art. 29 della direttiva n° 95/46/CE ha giudicato conforme alla direttiva stessa) al quale il presente codice si ispira.

Il suddetto Codice europeo di buona condotta, riprodotto in allegato, costituisce parte integrante delle disposizioni contenute nel presente codice.

Il codice è sottoscritto anche per le finalità indicate dall'art. 140 del D. Lgs. 196 del 30 giugno 2003 e nell'ambito del sistema di autodisciplina del settore individua i principi fondamentali della deontologia e della buona condotta. Esso quindi, a questo specifico fine e fermo restando il suo valore di codice di autodisciplina, espressione dell'autonomia privata dei soggetti che lo sottoscrivono, è sottoposto alle procedure di verifica di conformità alle leggi ed ai regolamenti previsti dall'articolo 12 del D. Lgs. 196 del 30 giugno 2003.

La sua sottoscrizione è effettuata ispirandosi alle pertinenti fonti e documenti internazionali in materia di attività di direct marketing, di vendita a distanza e di comunicazione interattiva e, in particolare:

- a) alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 4 novembre 1950, ratificata dall'Italia con legge 4 agosto 1955, n. 848;*
- b) alla Carta dei diritti fondamentali dell'Unione Europea del 18 dicembre 2000, con specifico riferimento agli artt. 7 e 8;*
- c) alla Convenzione n. 108 adottata a Strasburgo il 28 gennaio 1981, ratificata in Italia con legge 21 febbraio 1989, n. 98;*
- d) alla direttiva n. 95/46/CE del Parlamento europeo e del Consiglio dell'Unione Europea del 24 ottobre 1995 ed in particolare alle previsioni contenute nell'articolo 29 circa l'adozione di codici di deontologia e buona condotta ed alle successive norme dell'Unione Europea attinenti a questa materia;*
- e) alla Raccomandazione del Consiglio d'Europa n. R(85) del 25 ottobre 1985 (adottata nella riunione n. 389).*

Le società, gli enti, gli uffici e i soggetti che applicano il seguente codice prendono atto che i trattamenti di dati personali per finalità commerciali devono ispirarsi anche al principio di equo utilizzo dei dati nel pieno rispetto della volontà dell'interessato, oltre alle regole internazionali, comunitarie e nazionali in materia di trattamento dei dati personali.

Capo I – AMBITO DI APPLICAZIONE E PRINCIPI GENERALI

Art. 1 Ambito di applicazione

1. Le presenti norme sono volte a garantire che l'utilizzazione di dati personali acquisiti nell'esercizio della libertà di iniziativa economica e finalizzati allo svolgimento di attività di direct marketing, di vendita a distanza, di vendita diretta e di comunicazione commerciale diretta o interattiva si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, in particolare del diritto alla riservatezza e del diritto all'identità personale.
2. Il presente codice detta disposizioni per i trattamenti di dati personali effettuati a qualsiasi titolo per finalità commerciali, connesse direttamente o indirettamente alla vendita di prodotti o servizi, alla fidelizzazione di clienti e potenziali clienti ed all'invio di informazioni commerciali, nonché allo svolgimento di campagne di raccolta fondi effettuate a fini non profit. Il codice si applica all'insieme dei trattamenti di dati personali comunque effettuati per le suddette finalità.
3. Il presente codice individua, altresì, i principi e le linee guida di comportamento dei soggetti che trattano per le suddette finalità dati personali conservati presso archivi pubblici e archivi privati.

Art. 2 Definizioni

Nell'applicazione del presente codice si tiene conto delle definizioni e delle indicazioni contenute nella disciplina internazionale, comunitaria e nazionale in materia di trattamento dei dati personali e, in particolare, delle disposizioni citate nel Preambolo del presente codice. Ai medesimi fini si intende, altresì:

- a) per “**direct marketing**” qualsiasi attività di comunicazione indirizzata o non indirizzata quantificabile e pianificata, effettuata anche su sollecitazione dell'interessato, attraverso qualsiasi strumento di comunicazione conosciuto e che verrà sviluppato in futuro, il cui obiettivo principale sia creare o rafforzare una relazione diretta tra un soggetto economico o un ente non profit ed un soggetto individuato che acquista la qualifica di cliente, attuale o potenziale. Le attività di direct marketing possono avere tanto finalità commerciali quanto finalità non profit e di solidarietà sociali;
- b) per “**vendita a distanza**” il sistema distributivo nel quale il messaggio stampato, distribuito per posta o trasmesso per il tramite di sistemi telematici o audiovisivi, costituisce l'elemento principale od esclusivo per offrire prodotti e/o servizi alla clientela;
- c) per “**vendita diretta**” tutte quelle forme speciali di vendita che vengono effettuate mediante offerta di prodotti o servizi e raccolta di ordini dal consumatore finale, fuori dagli esercizi commerciali, da parte di imprese che si servono di *fiduciari di vendita*, altrimenti detti *incaricati*;
- d) per “**mezzi di raccolta dei dati**” gli strumenti attraverso i quali viene costituito un data base come ad esempio coupon, telefono, fax, e mail, internet, chioschi interattivi, questionari e schede la cui compilazione sia sollecitata o meno da informatori ed incaricati diretti;
- e) per “**cliente**” chiunque richieda, acquisti o utilizzi come destinatario finale un bene o un servizio;
- f) per “**prospect**” il cliente potenziale ed in generale chiunque non abbia già stabilito un rapporto commerciale con il titolare del trattamento;
- g) per “**lista**” o “**lista di marketing**” un data base contenente dati personali utilizzati per finalità di direct marketing, di vendita a distanza e di vendita diretta;

- h) per “**list broker**” il soggetto che effettua professionalmente o occasionalmente attività di fornitura o scambio di liste di marketing;
- i) per “**scambio di liste**” l’attività di comunicazione di dati, raccolti ed elaborati secondo le modalità previste dal presente codice, effettuata da due o più soggetti che reciprocamente mettono a disposizione, nel rispetto del principio di finalità del trattamento, una o più liste di marketing per l’effettuazione di attività di comunicazione commerciale;
- l) per “**terzi fornitori**” le società di telemarketing, le agenzie di marketing, le agenzie di promozione, i soggetti che effettuano attività di fulfillment, le società che effettuano servizi di postalizzazione ed in generale i soggetti che svolgono attività di trattamento di dati su richiesta del titolare per finalità strumentali alla realizzazione di una campagna di direct marketing;
- m) per “**comarketing**” l’attività di comunicazione commerciale diretta effettuata da due o più soggetti che indirizzano ad uno stesso destinatario messaggi contenuti in una medesima busta o inoltrati attraverso un medesimo supporto fisico o in un medesimo documento informatico o con un medesimo invio;
- n) per “**fidelizzazione**” l’attività volta a stabilire un rapporto continuativo con un cliente o con un potenziale cliente;
- o) per “**dati ad evidenza pubblica**” i dati personali di immediata e totale visibilità e liberamente conoscibili da chiunque, in quanto sono stati resi pubblici dall’interessato nella sua vita di relazione.

Art. 3 Modalità di comunicazione con l’interessato

Il presente codice si applica a tutte le attività di direct marketing, di vendita a distanza, di vendita diretta e di comunicazione diretta o interattiva con finalità commerciale o non profit effettuate mediante qualsiasi supporto, sia fisico che informatico, esistente o che verrà individuato in futuro, indirizzate a soggetti determinati o determinabili.

A titolo esemplificativo si indicano come strumenti di comunicazione diretta o interattiva:

- la corrispondenza postale
- la posta elettronica
- il telefono e gli SMS
- il fax
- le trasmissioni televisive interattive o che comunque determinino la raccolta di dati personali
- internet
- coupon
- materiale inserito nei pacchi destinati ai clienti o prospect
- spazi su giornali o riviste

fermo restando che le norme previste dal presente codice si applicano a qualsiasi forma di comunicazione diretta che determini, immediatamente o su iniziativa dell’interessato, un contatto diretto tra operatore e cliente o prospect.

Art. 4 Principio di precauzione

Nell’utilizzo delle liste di marketing i soggetti che effettuano attività di comunicazione diretta, con finalità commerciali o per perseguire fini non profit, si impegnano ad adottare il principio di precauzione al fine di prevenire ogni forma, anche per mera negligenza o imperizia, di illecito trattamento di dati personali. Pertanto gli operatori di direct marketing adotteranno qualsiasi cautela

per evitare l'accesso e l'utilizzo di liste di provenienza non definita e di cui non sia possibile ricostruire con certezza le modalità di formazione, con particolare riferimento al consenso al trattamento ed all'eventuale comunicazione dei dati.

Sulla base di tale criterio, applicando il principio di precauzione, gli operatori di direct marketing, di vendita a distanza e di vendita diretta si impegnano ad astenersi dall'uso di liste di cui non siano in grado di garantire, per conoscenza diretta o per espressa dichiarazione da parte del list broker o dell'azienda in co-marketing, la legittima provenienza ed il legittimo utilizzo.

A tal fine, ogni operazione di scambio di liste, o comunque di fornitura e di utilizzo di liste di marketing, verrà formalizzata mediante contratto che offra idonee garanzie circa la provenienza della lista e che dichiari il rispetto delle regole fissate dalla normativa vigente in materia.

Il mancato rispetto del principio di precauzione, accertato in concreto, costituirà criterio presuntivo, per affermare l'illegittimità del trattamento effettuato, salvo prova contraria.

Art.5 Principio del bilanciamento degli interessi

Nel rispetto della normativa vigente, i soggetti che effettuano attività di direct marketing, di vendita a distanza, di vendita diretta e di comunicazione diretta o interattiva beneficiano della clausola di esonero dal consenso dell'interessato, nel caso in cui sussista un legittimo interesse del titolare del trattamento o di un terzo al quale i dati sono comunicati, e non prevalga un diritto fondamentale o un altro legittimo interesse della persona interessata. Fermo restando che la determinazione dei criteri specifici per stabilire il bilanciamento di interessi viene definita dalle competenti autorità, come previsto dalla legge, gli operatori di direct marketing ispirano la loro condotta ai criteri di riferimento per la valutazione degli interessi perseguiti dalla loro iniziativa, così come sono definiti dalla direttiva comunitaria e dal Codice deontologico europeo, anche ai fini del trasferimento dei dati fra società collegate controllanti e controllate.

In particolare nel bilanciamento di interessi va tenuto presente che l'attività di direct marketing, di vendita a distanza e di vendita diretta:

- è espressione del diritto di libera iniziativa economica;
- è un'attività lecita;
- persegue finalità socialmente positive, in quanto offre prodotti e servizi attraverso tutti i canali di comunicazione (inclusi i canali alternativi a quelli tradizionali) e favorisce l'accesso a tali offerte da parte di tutti i soggetti.

Art. 6 Trattamento di dati sensibili

Tenuto conto della specifica normativa in materia di trattamento dei dati personali sensibili, è fatto divieto agli operatori di direct marketing, di vendita a distanza e di vendita diretta di discriminare i soggetti cui si riferiscono i dati trattati, in base ad informazioni che afferiscono alla sfera dei dati sensibili. Resta salvo il diritto dell'operatore economico di scegliere, nei limiti stabiliti dall'articolo 41 della Costituzione della Repubblica Italiana, a quali soggetti rivolgere le proprie offerte in base alle proprie libere politiche commerciali.

Capo II – INFORMATIVA, CONSENSO, COMUNICAZIONE DEI DATI

Art. 7 Informativa all'interessato

Ferme restando le disposizioni di legge, l'informativa da fornire all'interessato si ispira ai seguenti criteri:

- ove possibile viene formulata per iscritto, curando che la documentazione sia configurata in modo tale che all'interessato resti una copia dell'informativa stessa con l'indicazione delle modalità di esercizio dei diritti attribuiti dalla legge, qualora aderisca all'offerta formulata;
- è formulata con linguaggio chiaro, comprensibile, facilmente leggibile, utilizzando caratteri che per corpo e grafia risultino facilmente leggibili;
- viene riprodotta, ove possibile, in un sito internet nel quale siano fornite ulteriori indicazioni, sia sulla legge in materia di protezione dei dati personali, sia sul presente codice, sia sulla procedura aziendale adottata per garantire la massima riservatezza dei dati;
- contiene le indicazioni relative alle modalità di cancellazione dei dati ed in particolare allo specifico diritto dell'interessato di opporsi, in tutto o in parte, al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario, o di vendita a distanza o diretta, o di ricerche di mercato, o di comunicazione commerciale.

Nel caso in cui, tenuto conto della natura dello strumento di comunicazione utilizzato o per le caratteristiche personali e professionali dei soggetti destinatari del messaggio, il testo completo dell'informativa possa essere fornito anche attraverso l'accesso dell'interessato stesso ad internet, le notizie che l'interessato ha diritto di conoscere in base alla vigente normativa possono essere fornite in forma sintetica, rinviando per approfondimenti e precisazioni al testo riportato nel sito internet.

Qualora per esigenze di spazio non risultasse possibile fornire l'informativa completa, l'operatore di direct marketing, di vendita a distanza e di vendita diretta si impegna a fornire l'informativa sintetica e ad inviare l'informativa completa alla prima comunicazione commerciale successiva, ovvero ad inviarla su espressa richiesta dell'interessato, eventualmente anche con mezzi elettronici.

Questa stessa modalità semplificata di informativa è ammessa anche nel caso di comunicazione verbale effettuata attraverso il telefono.

Art. 8 Consenso

Il consenso reso dall'interessato per attività di direct marketing, di vendita a distanza, di vendita diretta o di comunicazione commerciale diretta o interattiva si intende riferito a tutti i trattamenti connessi direttamente od indirettamente all'effettuazione di comunicazione commerciale, alla vendita di prodotti o servizi strumentali allo svolgimento dell'attività, compresa la selezione della lista di marketing e la realizzazione e produzione del materiale necessario per effettuare la comunicazione diretta.

Pertanto il consenso reso dall'interessato per ricevere informazioni commerciali, offerte o promozioni si intende riferito all'intero trattamento, incluse le operazioni accessorie di verifica della correttezza e qualità dei dati utilizzati.

Il consenso reso per la comunicazione dei dati a terzi, per poter essere considerato validamente reso, deve far riferimento alle categorie di soggetti individuate in base al settore di attività che potranno ricevere tali dati.

In applicazione del principio in base al quale il consenso deve essere espresso liberamente e specificamente, la raccolta del consenso mediante formulari, tagliandi, coupon e cartoline o con strumenti telematici, può avvenire mediante l'apposizione di una frase prestampata che indichi chiaramente i contenuti e gli ambiti di tale consenso, lasciando all'interessato la libertà di manifestare la propria adesione o meno al consenso così formulato. Dovranno peraltro essere facilitate modalità che consentano all'interessato di modulare i contenuti del consenso, differenziandone gli ambiti di applicazione.

Il titolare del trattamento dovrà favorire l'esercizio del diritto di opposizione al trattamento ed il diritto di accesso ai dati, ove possibile creando procedure predefinite e strutture o servizi dedicati.

Ai fini della documentazione in forma scritta del consenso per il trattamento dei dati, i soggetti che utilizzano dati per finalità di marketing possono raccogliere il consenso degli interessati anche mediante dichiarazioni raccolte e sottoscritte da loro incaricati o addetti, purché tali attività siano sottoposte a specifiche regole di procedura e di controllo, effettuate a cura del titolare o di un suo responsabile.

Art. 9 Esecuzione dei lavori strumentali al trattamento e nomina dei responsabili del trattamento dei dati

Nell'esecuzione di operazioni strumentali al compimento di campagne di direct marketing, di vendita a distanza e di vendita diretta, laddove si renda necessario trattare dati personali avvalendosi di soggetti terzi, i quali assumono la qualifica di terzi fornitori su richiesta del titolare, lo svolgimento di tali attività deve avvenire in modo da garantire la massima riservatezza dei dati evitando abusi e utilizzi fraudolenti di tali liste.

A tal fine le modalità di trasferimento dei dati dal titolare ai terzi fornitori dovrà avvenire mediante una procedura formalizzata in base a regole definite preventivamente dalle parti.

Tali comunicazioni dei dati, disciplinate in base alla vigente normativa, potranno, a richiesta, essere rese note all'interessato, nel rispetto della riservatezza di informazioni afferenti all'attività aziendale.

Nei casi previsti dalla legge i terzi fornitori potranno essere nominati responsabili del trattamento, al fine di garantire la massima protezione dei dati personali anche nel loro flusso effettuato per ragioni produttive all'esterno dell'ambito aziendale. Tale nomina comporterà per il titolare l'onere di definire il livello di qualità del trattamento dei dati che il terzo fornitore dovrà impegnarsi a seguire e determinerà un onere di controllo e di vigilanza sull'operato del terzo fornitore.

A tale riguardo la scelta del fornitore va effettuata tenendo conto delle sue competenze professionali, delle strutture utilizzate e del livello di sicurezza offerto per garantire la protezione dei dati ricevuti per lo svolgimento dei servizi.

Ogni profilo di negligenza, di imprudenza o di imperizia nella scelta dei terzi fornitori comporterà la violazione del principio di precauzione prevista dall'articolo 4 del presente codice.

Capo III – SICUREZZA E REGOLE DI CONDOTTA

Art. 10 Modalità di raccolta dei dati

Nella definizione dei criteri di legittimità del trattamento dei dati per finalità di direct marketing, di vendita a distanza e di vendita diretta, ai fini del presente codice va tenuto conto tanto dello strumento di comunicazione utilizzato per inviare il messaggio, quanto della modalità attraverso la quale i dati vengono raccolti.

A tale riguardo, tenuto conto che la raccolta dei dati richiede verifiche e cautele di livello differente a seconda del luogo di raccolta e della fonte che fornisce le informazioni, si individuano i seguenti casi:

a) raccolta effettuata presso l'interessato

se i dati utilizzati per costituire una lista di marketing sono raccolti presso l'interessato, il titolare dovrà curare che, preventivamente ad ogni operazione di raccolta di informazioni, all'interessato vengano rese le notizie prescritte dalla legge in modo chiaro, comprensibile e preciso. Dovrà inoltre mettere a disposizione, su richiesta dell'interessato, ove sia stata predisposta, una documentazione integrativa che descriva la procedura aziendale di protezione dei dati personali.

b) raccolta effettuata presso terzi

se i dati utilizzati per costituire una lista di marketing sono stati raccolti presso terzi e quindi il titolare non ha avuto un precedente contatto con l'interessato, il terzo avrà cura di ricordare al titolare l'obbligo di fornire all'atto del primo contatto con il cliente o prospect le prescritte informazioni circa il trattamento dei dati stessi.

c) raccolta effettuata presso pubblici elenchi

se i dati utilizzati per costituire una lista di marketing sono stati raccolti presso una lista pubblica, al fine di consentire all'interessato di esercitare consapevolmente i suoi diritti di cancellazione e di opposizione al trattamento dei dati, il titolare, all'atto del primo contatto con l'interessato, indica la fonte dei dati. A tale riguardo si precisa che, entro i limiti indicati dalla vigente normativa, l'utilizzazione di dati ad evidenza pubblica, raccolti prima dell'entrata in vigore della legge è comunque consentita purché siano forniti all'interessato la possibilità di chiedere l'immediata cancellazione del suo nominativo dalle liste di marketing che il titolare ha intenzione di utilizzare.

Laddove la legge non precluda espressamente l'utilizzo di liste provenienti da pubblici elenchi, registri e albi conoscibili da chiunque, nel rispetto del principio di finalità, l'uso di tali dati per costituire liste di marketing sarà consentito una sola volta nell'ambito di una campagna di marketing al fine di ottenere il consenso al trattamento dei dati per quella specifica finalità. Qualora l'interessato non conceda il suo consenso al trattamento il titolare dovrà procedere alla cancellazione del dato, impegnandosi a non utilizzarlo ulteriormente per la medesima iniziativa di marketing.

Art. 11 Conservazione dei dati ed archiviazione del consenso

Nel rispetto delle regole fissate dalla normativa per la conservazione dei dati personali, gli operatori di direct marketing adottano tutte le cautele e cure per fare in modo che le informazioni contenute nelle liste di marketing siano custodite con diligenza ed ordine e siano facilmente organizzate in modo tale da permettere l'agevole esercizio dei diritti previsti dalla legge a favore dell'interessato.

L'archiviazione è effettuata in modo da consentire il tempestivo rinvenimento della dichiarazione di consenso dell'interessato e la sua esibizione a richiesta dell'interessato stesso o delle autorità.

È consentita l'archiviazione e la conservazione del consenso attraverso supporti informatici. In particolare l'archiviazione elettronica della dichiarazione del consenso, effettuata nel rispetto delle regole vigenti, è totalmente equiparata ad ogni effetto di legge, alla conservazione dei supporti originari e fa fede fino a querela di falso da parte dell'interessato.

La dichiarazione di consenso o la richiesta di cancellazione e di opposizione al trattamento stesso va conservata per il tempo previsto dalle normative vigenti ed in esecuzione di obblighi di legge.

Art. 12 Misure di sicurezza

In relazione alle misure minime di sicurezza previste dalla vigente normativa, il titolare del trattamento adotterà tutte le cautele necessarie in base al principio di precauzione e rispettando i specifici criteri di protezione dei dati, che avrà onere di individuare analiticamente, in particolare:

- a) il titolare del trattamento si impegna ad effettuare tutti gli investimenti necessari per garantire che la struttura organizzativa adottata protegga la riservatezza dei dati trattati;
- b) il titolare del trattamento, nel caso in cui si avvalga di persone preposte a qualsiasi titolo al trattamento dei dati, dovrà assicurarsi che questi soggetti adottino adeguate cure per la protezione dei dati sotto il profilo fisico, logico ed organizzativo;
- c) il titolare del trattamento dovrà esercitare un controllo costante sull'accesso al data base, definendo con appositi profili di autorizzazione le categorie di soggetti autorizzati all'utilizzo dei dati stessi.

Art. 13 Esercizio dei diritti dell'interessato e sistemi di cancellazione centralizzata

Nel rispetto della vigente normativa, nei casi in cui in base alla legge il trattamento non presuppone il consenso dell'interessato, gli operatori di direct marketing si impegnano a utilizzare preventivamente ogni forma di semplificazione che permetta ai clienti ed ai prospect di manifestare e rendere meglio conoscibile l'eventuale dichiarazione di non voler ricevere determinate comunicazioni.

In particolare gli aderenti al presente codice si impegnano ad utilizzare preventivamente tutte le liste di cancellazione centralizzata, i servizi di mail preference service e le liste robinson, che organizzazioni, associazioni ed istituzioni intendano mettere a disposizione ed il cui accesso non sia oneroso ed incompatibile con lo svolgimento della propria attività economica.

La sottoscrizione individuale del presente codice da parte dei singoli operatori di direct marketing, di vendite dirette e di vendite a distanza è requisito essenziale per applicare, sul materiale promozionale utilizzato per lo svolgimento della propria attività di comunicazione, il marchio della "Lista di cancellazione/Robinson List" adottata dalle singole associazioni che aderiscono al

presente codice, per favorire l'esercizio del diritto di cancellazione da parte degli interessati che non desiderano ricevere materiale promozionale.

Art. 14 Regole di condotta e procedura aziendale di protezione dei dati

Nel trattamento dei dati per finalità commerciali gli operatori si impegnano a seguire le seguenti regole di condotta, espressione del principio di precauzione indicato nel precedente articolo 4 del presente codice:

- a) evitare la duplicazione non necessaria dei dati;
- b) agire tempestivamente per la correzione e l'aggiornamento dei dati personali;
- c) eliminare prontamente dalla lista di marketing le persone defunte, non appena si abbia notizia di tale dato;
- d) nella definizione della lista di marketing fare in modo di adottare tutte le cautele per limitare il numero dei destinatari, in modo che l'offerta sia inviata ai soggetti effettivamente interessati a ricevere il messaggio;
- e) favorire la correzione delle liste di marketing utilizzate annotando le eventuali restituzioni degli invii postali per indirizzo errato o per dichiarazione di non recapitabilità effettuata dal vettore;
- f) informare gli interessati dell'esistenza di servizi di cancellazione centralizzata, di robinson list e di mail preference service;
- g) astenersi dall'utilizzo di liste la cui provenienza non sia garantita e certa;
- h) astenersi dal comunicare qualsiasi informazione che possa rivestire contenuto confidenziale, anche in presenza di consenso da parte dell'interessato, salvo che questo sia strettamente necessario per eseguire un'obbligazione o fornire un servizio aggiuntivo al cliente.

In particolare i titolari del trattamento si impegnano ad adottare dettagliate norme interne, definite attraverso un documento programmatico per la protezione dei dati personali, in esecuzione dei principi indicati dalla legge e da questo codice. Sarà cura del titolare del trattamento assicurare il rispetto delle regole di procedura e sanzionare al suo interno eventuali violazioni realizzate dai suoi dipendenti e collaboratori.

Capo IV – CASI SPECIFICI DI TRATTAMENTO DEI DATI PERSONALI

Art. 15 Raccolta e trattamento di dati per finalità di solidarietà sociale e non profit

Le attività di raccolta fondi e di fidelizzazione svolte dai soggetti che effettuano esclusivamente attività di solidarietà sociale e non profit avvengono nel rispetto del principio di finalità e tenuto conto delle specifiche regole stabilite a riguardo dalla normativa in materia di trattamento dei dati personali. Pertanto, ai fini del presente codice, l'utilizzo di strumenti e tecniche di direct marketing da parte di enti non profit non comporterà l'applicazione delle regole generali previste dalla normativa per il trattamento dei dati per finalità di comunicazione commerciali. Resta quindi inteso che i soggetti che statutariamente perseguono finalità di solidarietà sociale e non profit beneficiano in ogni caso delle regole di maggior favore previste dalla normativa vigente.

In particolare, nello svolgimento delle attività di raccolta fondi e di fidelizzazione dei donatori a favore degli enti non profit, la finalità di solidarietà sociale qualifica l'intero trattamento dei dati, indipendentemente dalla tecnica e dai metodi di comunicazione utilizzati.

Art.16 Telemarketing

Le attività di telemarketing e tutte le azioni di informazione commerciale effettuate per il tramite del telefono presuppongono la realizzazione di un'attività di formazione specifica attraverso la quale gli operatori telefonici siano messi in grado di fornire ai clienti e potenziali clienti con i quali entrino in contatto in modo chiaro, comprensibile e preciso, le informazioni relative al trattamento dei dati personali.

Di tale attività di formazione i titolari del trattamento ed i responsabili dei servizi di call center dovranno fornire apposita attestazione da conservare agli atti della società e da esibire a richiesta degli interessati e delle competenti autorità.

Il livello e l'approfondimento dell'informativa fornita agli interessati dovrà tener conto della natura *in bound* o *out bound* dell'azione di telemarketing.

Gli operatori telefonici che raccolgono il consenso orale dell'interessato e che lo documentano per iscritto sono resi edotti delle conseguenze pregiudizievoli, anche di natura penale, connesse all'attestazione di dichiarazioni false e non rappresentative dei fatti descritti. Di tale informazione i responsabili dei servizi di call center devono conservare apposita documentazione scritta.

Art 17 E-mail marketing

Nell'effettuazione di attività di comunicazione commerciale mediante la posta elettronica, i titolari del trattamento, nel rispetto della normativa vigente, si impegnano a contattare solo persone che abbiano fornito la loro non equivoca volontà di ricevere queste comunicazioni.

L'esistenza di un rapporto commerciale, contrattuale o precontrattuale con l'interessato autorizza l'invio di informazioni a mezzo della posta elettronica, salvo espresso diniego formulato dallo stesso interessato.

La definizione della mailing list dei destinatari di un messaggio di posta elettronica viene effettuata con criteri rigorosi, preventivamente determinati e controllabili, al fine di evitare l'invio di messaggi indesiderati e non sollecitati.

Non è in ogni caso consentito l'invio di messaggi ad indirizzi generati automaticamente senza il preventivo consenso degli interessati, neppure ove tale generazione della lista di marketing risponda a criteri predefiniti e rigorosi.

L'invio di qualsiasi tipo di messaggio telematico, inclusa la posta elettronica, per effettuare comunicazioni commerciali ad una generalità di destinatari, la cui lista non sia stata formata attraverso criteri univoci e predeterminati, non rientra tra le attività di direct marketing, di vendita a distanza, di vendita diretta e di comunicazione interattiva in quanto si fonda su presupposti estranei a questa attività e viola lo spirito al quale si ispirano le azioni oggetto del presente codice.

Art.18 Vendite a distanza e commercio elettronico

Nelle attività di vendita a distanza e di commercio elettronico, nei limiti delle disposizioni previste dalla vigente normativa internazionale, comunitaria e nazionale, l'esistenza di trattative precontrattuali, contrattuali e la fornitura di servizi post-vendita e di assistenza, presuppone che

possano essere inviati messaggi all'interessato al fine di proseguire il rapporto commerciale e di fidelizzare il cliente.

Pertanto, ove sia affermata l'esistenza di tale situazione negoziale, il titolare del trattamento sarà libero di inviare messaggi informativi all'interessato, purché non comportino oneri a carico del destinatario e a patto che in ogni comunicazione l'interessato riceva apposita informazione dei propri diritti di cancellazione ed opposizione al trattamento e venga messo in condizioni di esercitarli in modo agevole.

La liceità delle comunicazioni dirette finalizzate alla vendita a distanza è valutata anche alla luce delle norme di autodisciplina, deontologiche e di buona condotta emanate dalle organizzazioni maggiormente rappresentative del settore in ambito internazionale e nazionale.

Capo V – SISTEMA DI CONTROLLO ED APPARATO SANZIONATORIO

Art. 19 Autorità di controllo ed autodisciplina

OMISSIS

Art. 20 Norme di procedura e sistema sanzionatorio

OMISSIS

Milano, 15 Dicembre 2003

Appendice A

~~Codice Europeo di buona condotta per il trattamento dei dati personali nel direct marketing~~ **ALLEGATO A**



FEDERATION OF EUROPEAN DIRECT MARKETING

EUROPEAN CODE OF PRACTICE FOR THE USE OF PERSONAL DATA IN DIRECT MARKETING

EXPLANATORY MEMORANDUM

FEDMA represents the direct marketing sector at the European level. Its national members are the Direct Marketing Associations (DMAs) of 12 countries of the European Union (all except Belgium, Luxembourg and Denmark) and Switzerland, Norway, Hungary, Poland, the Czech and Slovak Republics, which represent users, service providers and media/carriers of direct marketing. FEDMA also has about 350 direct company members.

Representing directly, or indirectly through the trade associations, a total of around 10,000 European direct marketing practitioners, FEDMA is ideally placed to draw up a European data protection code of practice for practitioners, which it has prepared following discussions with the Article 29 Group. This essential instrument represents an interpretation of the European Data Protection Directive in terms designed to be understood by direct marketers; in some areas of the Directive where practice already goes beyond the level set by the Directive – or where FEDMA recommends that it should – such higher standards of practice are incorporated.

All the national members of FEDMA, i.e. the trade associations, have agreed that their own national codes will in every respect maintain levels of protection for data subjects at least as high as those provided by the FEDMA Code, although – where national laws or self regulation oblige or allow – their national code may reflect even higher standards.

The code is designed primarily as an instrument of best practice, and it is intended for use as a reference document within the framework of applicable laws. Direct members of FEDMA will operate to the standards laid down in the FEDMA Code, subject always to their obligation to comply with their relevant national laws or self-regulatory provisions. This code is not intended to reduce or replace the applicability of national laws and regulations.

FEDMA hopes, and will actively promulgate the view, that the FEDMA Code should also be regarded by all European direct marketing practitioners – whether members or not – as the general standard or custom and practice for the Industry as a whole.

It is also accepted by FEDMA that this Code of practice is merely the first stage in the ongoing development of effective best practice in the area of data protection. As subsequent editions of the Code become more sophisticated and continue to mirror the best and ever increasing aspirations of responsible practitioners, so will Industry practices across the board be raised to levels constantly matching the legitimate and growing expectations of the Industry's customers.

It is as well to remember that the data protection legislation applies to the processing of personal data using any medium.

It should be noted that different means of communication used by direct marketing have attracted different regulations. Directives 97/66/EC (Telecommunication and Privacy) and 97/7/EC (Distance Selling) require the consent of the data subject before a commercial communication can be sent to him/her by fax or automatic calling unit. Directive 2002/58/EC (Privacy and Electronic Communication) in addition requires that consent is needed before using electronic communications (e.g. e-mailing) to consumers who have no previous relationship with the data controller.

This code should be read in conjunction with the other FEDMA existing and forthcoming codes of practice, including the European principles for the use of the telephone as a marketing medium by business, and The Electronic Commerce Code of Conduct for European Business. This code should also be applied with the Global Conventions on Mailing and Telephone Preference Services and the Global E-mail Preference Service principles¹.

The code is designed to be applied to the use of personal data by direct marketers within the EU and those non-EU countries², which have national data protection laws in line with the EU Directive.

All provisions of this code apply without prejudice to the provisions of the applicable national legislation. Where specific requirements exist at national level, this will have to be complied with in accordance with the applicable law rules set out in this Code and in accordance with EU legislation.

1 The Global Conventions on Preference Services, FEDMA code of conduct for electronic commerce and the European principles for the use of the telephone as a marketing medium by business can be accessed at FEDMA. Information on the Global Email Preference Service can be found at <http://www.e-mps.org>. Robinson lists equal Preference Services (see footnote page 11).

2 EEA and other European countries which national data protection legislation is considered as providing an adequate level of protection.

DEFINITIONS

DIRECT MARKETING

The communication by whatever means (including but not limited to mail, fax, telephone, on-line services etc...) of any advertising or marketing material, which is carried out by the Direct Marketer itself or on its behalf and which is directed to particular individuals.

PERSONAL DATA

Personal Data means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Note

Personal Data means information relating to an individual, held in a form in which the individual can be identified, and could include as little as a surname. Some information not containing a surname should be considered as Personal Data and therefore covered by this code. This could be the case, for example, in regard to postal addresses, telephone numbers, faxes or e-mail addresses, or job title, if the person to whom these data relate can reasonably be identifiable by the Data Controller.

SENSITIVE DATA

Any data which reveals any of the following information from a Data Subject is sensitive and is subject to restrictions on their processing:

- Racial or ethnic origin;
- Political opinions;
- Membership of a trade union;
- Religious or philosophical beliefs;
- Physical or mental condition (health);
- Sexual life;
- Offences, criminal convictions and security measures.

DIRECT MARKETER

Any natural or legal person (including charities and political parties) who communicates by whatever means (including but not limited to mail, fax, telephone, on-line services etc...) any advertising or marketing material which is directed to particular individuals.

DATA SUBJECT

The individual for which Personal Data can be identified or identifiable.

DATA PROTECTION CO-ORDINATOR

Any natural person appointed by the Data Controller to undertake the functions described in this Code.

DATA CONTROLLER

For the purposes of this code, a Data Controller means any natural or legal person who determines and controls (jointly or in common with other natural or legal persons) the purposes and the ways in which processing of Personal Data is, or is to be undertaken.

Note

A Data Controller must not be confused with a data owner. For example, an organisation can be the data owner of a database (because that natural or legal person is in possession of the material rights to use the database) and at the same time the Data Controller of the processing.

DATA PROCESSOR

Any natural or legal person, other than an employee of the Data Controller, who processes Personal Data exclusively under the instructions, responsibility and on behalf of the Data Controller.

THIRD PARTY

Any natural or legal person who is neither the Data Subject, nor the Data Controller, nor the Data Processor, nor the agents/employees of the Data Controller or the Data Processor.

Note

A Data Controller may appoint company A as their Data Processor. The Data Processor can only process the data following the instructions of the Data Controller. However, if the Data Controller decides to rent a specific list to company B, this company will be a Third Party.

PROCESSING

For the purpose of this code, processing means any automated operation performed upon Personal Data for Direct Marketing purposes. Manual operations are also covered when they are performed in a structured way according to specific criteria and which will permit easy access to the data.

Note

The term covers each of the separate chain of operations that an organisation may do with the Personal Data from the first collection until the destruction, and including any other intermediary operations such as rectification, maintaining, storing and disclosure. This code only applies to processing related to Direct Marketing activities. Marketers should also check that the other types of processing carried out by them also comply with the applicable data protection rules.

DISCLOSURE

Any communication (provision or making available) of Personal Data (e.g. renting, selling) to Third Parties.

CHILDREN

Any individual aged under 14 years old unless otherwise defined in national legislation/self regulation

PARENT

The Child's parent or legal guardian

1 Law applicable

1.1 Direct Marketers established in EU/EEA territory

When the Direct Marketer is established in the EU/EEA area, in order to know which national law they have to respect, they have to take into consideration the following rules:

- 1.1.1 If the Direct Marketer has just one establishment in the EU/EEA and therefore one single Data Controller, the law applicable is the one where the Data Controller is established, subject to the rules set out in point 1.1.4.
- 1.1.2 If the organisation has different establishments located in different EU/EEA members and if one and only one of these establishments is to be considered as the Data Controller whereas the other establishments are just processors, each processor should respect the national law of the Data Controller except with respect to security measures for which the processor has to follow its national law.
- 1.1.3 If the Direct Marketer has different establishments located in different EU/EEA member states and each of them acts as a Data Controller, each establishment should respect the national laws of the country where they are established.
- 1.1.4 If the Direct Marketer acting as the Data Controller uses a processor agent located in a different EU/EEA member state, the processor agent has to apply the law applicable to the EU-established Data Controller, except in relation to security measures provisions in which case the law of the country where the Data Processor is established should apply.
- 1.1.5 The fact that the data are from natural persons of one or more EU/EEA countries or from countries outside the EU/EEA area is not a determining factor in the designation of the law applicable.

The different possible situations are summarised, for practical reasons in the following matrix:

CASES	FACTS				LAW APPLICABLE	
	Direct Marketer established in	Data Controller established in	Data Processor established in	Data from	To <u>the</u> <u>respective</u> processing	To security measures
1 st	BE	BE	BE	EU EEA US	BE	BE
2 nd	BE NL UK	BE	NL UK	EU EEA US	BE	NL UK
3 rd	BE	BE NL UK	FR	EU EEA US	BE NL UK	FR
4 th	BE	BE NL UK	SP PT LUX	EU EEA US	BE NL UK	SP PT LUX

1.2 Data Controllers not established in the EU/EEA territory

When a Data Controller is not established in the EU/EEA it would have to respect the national law of one of the Member States of the EU/EEA when, for the purposes of processing, it used equipment situated in one of those Member States (for example, a call centre to collect Personal Data, a bureau to process Personal Data on their behalf, a list broker to update their lists, etc). In this case:

- 1.2.1 The Data Controller should designate a representative (natural or legal person) that is established in the Member State in which such processing takes place. The representative will be responsible vis-à-vis the competent national authorities to guarantee that the national law

applicable is respected by the Data Controller. (This does not mean that the authorities cannot initiate legal actions against the controller itself.)

- 1.2.2 The law applicable would be the one where the representative is established.
- 1.2.3 The provisions of article 1.2 are not applicable if the equipment is used only for transit purposes within the EU/EEA (for example, if the Data Controller is established in Canada, the data are collected in countries outside the EU/EEA territory, then sent via a UK telecommunications service provider to Canada).

2 Obtaining Personal Data

2.1 Collection directly from the Data Subject

Whilst collecting data, the Data Controller should ensure that the collection is done in a fair manner and that the Data Subject's right to information, as outlined in this code, is secured.

General principles for fair processing

- *Essential Information*

Data Controllers must ensure that Data Subjects are informed of:

- the identity of the Data Controller (e.g. name and address);
- the purpose(s) of the processing (e.g. transactional or promotional purposes)

The essential information should be given at the time of the collection, unless it is completely clear from the context (for example, as regards the identity of the controller and the purpose, if the name of the company is clearly shown in the promotion), or the Data Subject already has the information (for example, if the Data Subject has a contract with the company).

- Information on the rights to access and correct *data* and objections

Data Controllers must ensure that Data Subjects are informed of:

- their right to access and correct erroneous data related to them;
- their right not to be approached for Direct Marketing purposes;
- their right to object to the processing of his/her Personal Data for Direct Marketing purposes.

Treating with specific situations

- *Information in the case of data used for the controller's Direct Marketing activities*

In the case where the data are intended to be used by the controller for its own Direct Marketing use, the Data Controller must ensure that the Data Subject is aware of the essential information, and of his/her right to opt-out from such use.

The Data Controller should provide the information at the time of collection and every effort should be made to do so. But in the case where this is difficult or impossible (i.e. small space advertisements or telemarketing) and permitted by national legislation this information may be given as soon as possible after the collection, for example, when the Data Subject receives the first documentation (invoice, receipt, etc.) in written or any durable medium.

- *Information in the case of disclosure*

In addition to the essential information, when data are intended to be communicated to Third Parties, Data Controllers must ensure that Data Subjects are informed of:

- any recipients or types of recipients of the data and the purpose for which the data will be disclosed;
- their right to object to from disclosing for Direct Marketing purposes

This information should be given at the time of collection, and every effort should be made to do so, but where this might be difficult or impossible (for instance in case of small space advertisements or telemarketing) and it is permitted by national legislation, this information should be given before any such communication to 3rd parties takes place.

This information may not need to be provided if it has already been given through appropriate mechanisms (e.g. appropriate collective notice which is generally accessible and sufficiently targeted

to a specific public). Such mechanisms must be permitted by national legislation and should be conveyed in accordance with the legal requirements contained in the applicable national legislation.

- *Information in the case of use of questionnaires and other forms*

In addition to this essential information, Data Controllers must ensure that Data Subjects are informed of whether the replies to questions are obligatory or voluntary, and the possible consequences of a failure to reply (for example, including but not limited to, situations of not receiving a gift in the case of collection of data by means of questionnaires). The Data Controller should also ensure that no unnecessary questions are asked.

The information in the case of questionnaires should be given at the time of collection.

2.2 Collection from sources other than the Data Subject

2.2.1 Where Data Controllers do not collect Personal Data from the Data Subjects themselves, they are obliged to take such steps as are necessary to ensure that the Data Subjects are nevertheless aware of the information they would have had if direct contact had been made with Data Controllers. For example rented-in lists, member-get-member campaigns, or data collected from questionnaires must in particular be in conformity with the principles of legitimacy as defined in Article 2.1.

2.2.2 Data Controllers should provide the information referred to in Article 2.1:

- at the time of undertaking the recording (i.e. processing) of the data;
- or, where the disclosure to a Third Party is envisaged, no later than the time of disclosure, providing such disclosure takes place soon after the data is recorded (processed).

2.2.3 Providing that the data used were initially collected respecting data protection rules, as a derogation to the principles set out in Article 2.2.1, the above requirement does not apply in specific exceptional circumstances where it would involve a disproportionate effort to provide such information, and where any additional appropriate safeguards, as laid down in national law, are met. In particular, circumstances which involve disproportionately high expenditure in terms of time or money. E.g. when data are obtained from a 3rd party and are to be used after a short time delay, it would be disproportionate directly to inform the Data Subject, when it can wait until first contact takes place.

2.2.4 These factors will always need to be balanced against the consequences to the Data Subjects arising from an application of the derogation. Examples of circumstances where the disproportionate effort derogation might, all other things being equal, be applicable would include:

- Personal Data held for the purposes of blocking or address verification;
- where Personal Data are suppressed by application of a Robinson List or Preference Service File;
- where a marketer removes or suppresses the Personal Data of those on the marketing list which do not match the required profile.

2.2.5 Data Controllers, having assessed the relevant factors and having decided to apply the derogation, should ensure that a written statement (setting out the reasoning underlying the decision, the type of information that the Data Controllers would have had to give, and why the Data Subjects would not be prejudiced by the application of the derogation) is prepared and is available subsequently in justification of such decision.

2.3 Collection of Sensitive Data

Due to the particular importance of Sensitive Data with regard to the Data Subject's fundamental privacy rights, special care needs to be taken in the processing of such data.

If the Personal Data being collected involves Sensitive Data, the Data Controller must request the explicit consent of the Data Subject for the collection and further processing of the Personal Data. Explicit consent means specific, freely given and informed in such a way that there should be no doubt at all concerning the consent of the Data Subject that should undertake action in order to make his/her consent clear. Explicit consent does not necessarily mean in writing but it is often the case in practice as this constitutes a good means of proof of the consent unless:

- the data have been manifestly made public by the Data Subject (for example, in the case of information from a public source such as a directory, where the Data Subject has been given the opportunity not to include those data), or;
- the data are processed by a relevant non-profit organisation with a political, philosophical, religious or trade-union aim. If these organisations process data without the explicit consent of the Data Subject they must take into account that:
 - the processing should be carried out in the course of the legitimate activities of these bodies;
 - appropriate guarantees should be offered;
 - the processing may only relate to the members of the body or to persons who have regular contact with it;
 - the processing should take place in connection with the purposes of the non-profit-seeking body;
 - the data are not disclosed to a Third Party without the consent of the Data Subjects.

An example of this kind activities could be a church or religious association that sends (or uses a processor to send) a letter to its members announcing the publication of a religious bulletin to which interested members could subscribe, or to raise funds for providing help and assistance in a specific situation.

Under no circumstances should companies use Sensitive Data in a way which may prejudice the fundamental rights and freedoms of the Data Subject. Data must always be processed for legitimate activities.

Where sensitive data, collected in connection with Direct Marketing activities, are processed further for statistical analysis purposes, they should be made anonymous or at least transformed in such a way as not to allow identification of data subjects, unless the Data Controller has obtained the Data Subject's explicit consent.

2.4 Different purposes

2.4.1 If one intends to process Personal Data for a purpose significantly different than that for which the data were originally collected the Data Controller should check if the new purpose is compatible with the notified purpose. If it is compatible, processing for this new purpose is allowed. In the case the new purpose is incompatible with the notified purpose, further processing is only allowed if it is in accordance with applicable data protection laws.

2.4.2 In assessing the compatibility of the new purpose, Data Controllers should among others aspects take into consideration the following criteria: whether the new purpose(s) is substantially different from the purpose(s) for which data were collected, whether Data

Subjects could reasonably have foreseen or whether it is probable that they would have objected to if they had known. The Data Controller should always take into account relevant national legal guidance issued by the relevant national Data Protection Authority.

2.5 Host Mailings

If Data Controllers make a host mailing exclusively on the basis of selective criteria, they must inform the Data Subject of this, otherwise Data Controllers might divulge Personal Data to Third Parties without realising they were doing so.

Host mailings are when a Data Controller encloses Third Party material in its mailings. Selective criteria in this context means criteria which could have a detrimental effect on the rights of the Data Subject – for example, the use of sensitive data linked to a sales pattern (past purchases of a pharmaceutical product for example). This provision suggests that the Data Controller should ensure the Data Subject is informed in the host mailing letter as the most effective means available to inform.

2.6 Specific provisions for Children

2.6.1 In collecting Children's data, Data Controllers should always make every reasonable effort to ensure that the Child and/or the Parent are properly informed about the purposes of the processing of the Child's data.

In particular when using commercial materials directed at Children or otherwise knowingly collecting data from Children, the information notice should be prominent, readily accessible and understandable by Children.

2.6.2 Whenever applicable national or European data protection law requires the Data Subject's consent to the processing, Data Controllers must obtain the informed and prior consent from the Child's Parent. The form and the method in which consent must be obtained should always comply with applicable laws and self-regulation.

2.6.3 Data Controllers should give the Child's Parent the same rights over the Child's data as those described in section 3.5 of this code. Data Controllers should use every reasonable endeavour to verify that the person that exercises the Child's right is the Child's Parent.

2.6.4 Data Controllers should not make the Child's participation in a game, the offering of a prize or any other activity involving a promotional benefit conditional on the Child disclosing more Personal Data than what is strictly necessary for the participating in such activity.

3 Responsibilities of the Data Controller

3.1 Data Protection Principles

- 3.1.1 Data Controllers must comply with the following principles: Personal Data must be
- processed fairly and lawfully on the basis of a legitimate ground (in accordance with the applicable law and the provisions of this Code);
 - collected for specified explicit and legitimate purposes (e.g. the purposes declared to the Data Protection Authority such as trading in personal information, distance selling operations);
 - not further processed in a way incompatible with those purposes³ unless the Data Subject has given his/her further consent;
 - adequate, relevant (e.g. it is normal for an air company to ask passengers about their eating habits in order to give them the right kind of meals but a car company does not normally need to know about the eating habits of its customers because they supply clients normally no meals), and not excessive in relation to the purposes for which they are collected and/or further processed;
 - accurate and kept up to date. This can be done through the use of suppression lists (both in-house and General Robinson Lists⁴), publicly available data and the right to rectification exercised by the Data Subject.
 - kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the data were collected and for which they are further processed.
- 3.1.2 Controllers should have a contract with their processors by which the processor agrees to comply with those principles, and to act only on the instructions of the controller. The responsibility for fair and lawful processing remains with the controller and cannot be transferred to a processor by means of a contract.

3.2 Notification to the Data Protection Authorities

Data Controllers should ensure that their processing operations are registered according to the appropriate law applicable.

3.3 Security Measures

- 3.3.1 Controllers should ensure that they employ appropriate security measures, having regard to the cost and the technology state of the art for their implementation and to the sensitivity of the information, to prevent accidental and unlawful destruction or accidental loss, alteration and unauthorised disclosure or access of their Personal Data files. For further safeguard, controllers are encouraged to use specific measures, such as Privacy Enhancing Technologies (PETs), and seeding lists. The written convention between the list-broker and the list user should ensure that lists are used with respect to appropriate security principles.
- 3.3.2 Such measures include, among others, security of the buildings in which the Personal Data are stored and/or processed (including access to the building), list of authorised persons (with a mention of their liability) to access the data, appropriate authentication mechanisms (e.g. passwords control), and security in the transfer of data between the Data Controller and the Data Processor.

³ See the examples mentioned in article 2.4.1 above.

⁴ Robinson lists equal Preference Services.

- 3.3.3 Controllers can refer to their national Direct Marketing Associations for guidance on appropriate security measures and state of the art technology.
- 3.3.4 Controllers should satisfy themselves that any processors they employ have appropriate security measures (including respect for confidentiality) by including appropriate provisions in the contract mentioned in article 3.3.1.

3.4 Contact point

- 3.4.1 Controllers should designate a Data Protection Co-ordinator within the organisation acting as a contact point for relevant data protection issues.
- 3.4.2 The functions of the Data Protection Co-ordinator should at least include:
- monitoring alone or with someone else the compliance of the organisations data protection practices with the applicable law and the provisions of this Code;
 - acting as a contact point for the relevant Data Protection Authority/ies
- 3.4.3 The national DMAs may wish to collect the names of the Data Protection Co-ordinators of their members for transmission to the relevant Data Protection Authority.

3.5 Exercise of the Data Subjects' rights

In addition to comply with the principles set out in 3.1, controllers should comply with all the Data Subjects' rights as defined in this code and in applicable legislation, including the right to:

- object to the processing of his data for Direct Marketing including the possibility of not being contacted on behalf of someone else. Holding data for the purpose of blocking Direct Marketing communication would not be considered as Direct Marketing processing;
- object to the disclosure of data to a Third Party, except in cases where such disclosure is required by national legislation;
- access and to rectify data which are inaccurate in accordance with Article 4.1 and 4.2 of this code;
- claim the deletion or blocking of data when its processing does not comply with the provisions of the applicable legislation;
- object on legitimate compelling grounds to the processing of data for purposes other than Direct Marketing, unless otherwise provided in the applicable legislation.

3.6 Disclosure of lists

- 3.6.1 Data Controllers who disclose their list to other organisations should take reasonable steps (e.g. request an example of the material) to investigate the intentions of the use the data will be put to (e.g. whether the content of the material may be illegal, unethical, or likely to harm the image of Direct Marketing in general, or contain material which is unacceptable, such as pornography).
- 3.6.2 Data Controllers (for example, list brokers) should also have an agreement evidenced in writing with the prospective user (Third Party) by which it undertakes to abide by the principles of this Code, before disclosing data.

4 Dealing with Data Subjects' requests

4.1 Access to data

4.1.1 Every Data Subject has the right to obtain from the controller:

- confirmation as to whether or not data relating to him/her are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed.
- communication to him/her in an intelligible form of the data undergoing processing and any available information as to their source.
- knowledge of the logic involved in any automatic processing in the case of automated decisions⁵.

4.1.2 Controllers who receive requests, in writing or in any other durable medium, from Data Subjects to see the Personal Data held on them should:

- indicate any special information which might be needed from those Data Subjects, in particular his/her identity, in order to ensure that the Data Subject is duly entitled to exercise the right of access as well as to locate their records (e.g. mailing campaign reference);
- supply the Personal Data in a readily intelligible form and enclose any notes or explanations to cover any ambiguous information, for example, a list of codes applied by the Data Controller;
- inform them about any reasonable charge they intend to make for supplying the data, if allowed by national law, such fee should not exceed the maximum limit laid down by national regulations;
- inform them of the logic involved in any automatic processing of data concerning him/her for the purpose of evaluating matters relating to him/her such as, for example, the Data Subject's creditworthiness.

4.1.3 Controllers are not obliged to answer requests that are made at unreasonable intervals (as defined in national applicable laws and/or codes of conduct which provide more protective measures).

4.2 Rectification

Data Controllers should act on any request, in writing or in any other durable medium, for rectification of the Personal Data. If there are compelling grounds for doubting the legitimacy of a request for rectification, further proof should be required before proceeding to the rectification. This can, for instance, be the case when the request comes from a minor without the Parents' or guardian's approval, or if the Data Controller holds information that shows that the request to amend the data is not justified. For instance, if a Data Subject says that he/she has never ordered a product by a given company and this company has evidence of this purchase.

Compelling legitimate grounds also exist when there are sufficient reasons to believe that the request is excessive. This can for instance be due to the frequency of the request.

When no rectification is justified the Data Subject should be informed about this decision.

⁵ Automated individual decision means any decision which produces legal effect on the data subject or significantly affects him and which is based only on automated processing for the purpose of evaluating him or her such as for example the data subject creditworthiness. Automated individual decision processing can only be used in accordance with national relevant legislation.

4.3 Source of the data

When Data Controllers receive requests, in writing or in any other durable medium, from Data Subjects enquiring about the source of their Data Controllers should, where it is lawful and where the source can be identified by reasonable efforts, communicate the information to the enquirer. If data has been compiled from different sources, Data Controllers are encouraged to keep a list of sources from which Personal Data have been obtained.

4.4 Timing for dealing with Data Subject requests

4.4.1 Data Controllers should supply the information required in articles 4.1, 4.2 and 4.3 in a short period, which should not exceed the period allowed by applicable national rules.

4.4.2 FEDMA recommends that controllers supply such information within 20 working days, unless there are exceptional circumstances.

5 Preference Services Systems

5.1 In-House Suppression Lists

- 5.1.1 Data Controllers should ensure that a suppression system, to block names (or other relevant identification details, e.g. telephone numbers or e-mail addresses, see note on Personal Data in the Definitions) of Data Subjects who have requested not to be approached for Direct Marketing, operates in their databases.
- 5.1.2 If Data Controllers receive a request not to approach a Data Subject by whatever means, they should as soon as possible and at least in no more than 4 weeks of receiving that request, have blocked that Data Subject's name in their databases.
- 5.1.3 Data Controllers responding to a Data Subject's "do not promote" request should explain that the suppression may not apply to Direct Marketing material which may have been prepared before the request was received. Data Controllers should take all reasonable measures to ensure that the Data Subject does not receive further Direct Marketing material as soon as possible and at least in no more than 3 months after receiving the request.

5.2 Preference Services Systems

- 5.2.1 Data Controllers should subscribe to the principles of national Preference Services⁶ where these operate, and when using Personal Data from other countries in which such services operate, regularly clean their lists against the preference services, in accordance with the Global Conventions on Preference Services. The DMAs in charge of the Preference Services must regularly clean their files.
- 5.2.2 Suppression requests are kept in preference services systems for at least a period of three years or, such greater period as established by the national regulations on preference services systems. In the specific case of e-mail preference services, files may have to be updated within a shorter period than three years, in accordance with national regulations on e-MPS.

An up to date archive of suppression requests must be maintained for a minimum period of three years or, such greater period as established by national regulations or the national preference service. In the specific case of e-mail suppression requests, a shorter period will be acceptable where national regulations or e-mail preference services allows.

The owner or manager of the preference service system should inform the Data Subject about the time period for which the request is valid, for example, when the Data Subject receives the confirmation of his/her suppression request.

⁶ These Preference Services can include Mailing Preference (Robinson Lists), Telephone Preference, Fax Preference or E-mail Preference Services. Note, however, that the Data Controller must also comply with the need for consent when using Automatic Calling Machines and Faxes in accordance with Directive 97/66/EC (Telecommunication and Data Privacy Directive), as well with the provision that are set out for electronic communications in accordance with Directive 2002/58/EC (Directive on Privacy and e-Communication).

6 Transfers of Data to non-EU countries

In case of transfers to non-EU/EEA countries which are not considered as having an adequate level of protection⁷, the Data Controller can only transfer personal data if sufficient safeguards are provided, by drawing up a contract (often this needs to be approved at national level), or by providing any other forms of mechanisms endorsed by the EU, unless the Data Subject has given his/her unambiguous consent, or the transfer is necessary for the performance of a contract between the Data Subject and the controller, or the implementation of precontractual measures taken in response to the Data Subject's request.

⁷ The list of countries considered as having adequate protection and the procedure provided by the European Commission and the national Member States must be used.

7 Compliance and Monitoring

7.1 Responsibility of the national DMAs

The national Direct Marketing Associations are responsible for the strict application of the principles set up in this Code, as incorporated into their national codes, in their respective countries and should apply the same sanctions stipulated in their countries for the breaching of their national codes.

Companies should regularly monitor their compliance to this code (for example, via self-audits).⁸

7.2 Resolution of complaints

7.2.1 National Direct Marketing Associations should establish a procedure to solve any complaints that may arise from the application of this Code at national level.

7.2.2 National Direct Marketing Associations should nominate a person within the association responsible to handle the complaints and to act as the contact person for FEDMA. The name of this person should be communicated to the relevant Data Protection authority.

7.2.3 If a national Direct Marketing Association is unable to solve a complaint from a Data Subject due to its cross-border aspects, it should refer the matter to FEDMA, which should nominate a person within the Federation responsible for the resolution of complaints.

7.2.4 The national DMAs should co-operate as much as possible with their national data protection authorities.

7.2.5 FEDMA will also co-operate with other relevant organisations and government bodies.

7.3 Contravention of the principles

7.3.1 Any contravention of this Code by FEDMA members would be brought to the FEDMA Data Protection Committee for consideration. The Data Protection Committee, taking due regard to the type of contravention, may decide to recommend to the FEDMA Board the expulsion of the member or other sanctions, according to its rules of procedure.

7.3.2 FEDMA may consider the possibility of initiating action against a member or a non-member in order to safeguard the ethics of the profession⁹.

7.3.3 The non-compliance with the provisions of this Code may also result in specific legal actions from the national data protection supervisory authorities.

7.4 Data Protection Committee

⁸ Checklists elaborated by the Data Protection Authorities should be taken into account.

⁹ E.g., in Belgium professional organisations can initiate actions on these grounds.

- 7.4.1 A Data Protection Committee is established within FEDMA to monitor the application of the FEDMA Code. The Data Protection Committee reports to the FEDMA Board.
- 7.4.2 The Data Protection Committee is composed by the contact persons of the national DMAs as established in article 7.2.2; the nominee contact point within FEDMA; and three representatives from companies who should be members of the FEDMA Board.
- 7.4.3 The functions of the Data Protection Committee are:
- to consider annually if a revision of the Code is necessary;
 - to provide the Article 29 Working Party with an annual report on the functioning of the code at national level and in cross-border activities;
 - to solve cross-border complaints in co-operation with the IFDMA (International Federation of Direct Marketing Associations) and EASA (European Advertising Standards Alliance);
 - to consider any contravention of the Code.
- 7.4.4 The Data Protection Committee should adopt its internal rules of procedure.