## НАШ СПІВРОЗМОВНИК
## ТАРАС КОПИТЬКО,
### ПРЕЗИДЕНТ УКРАЇНСЬКОЇ АСОЦІАЦІЇ ДИРЕКТ МАРКЕТИНГУ, ГЕНЕРАЛЬНИЙ ДИРЕКТОР АГЕНЦІЇ ПРЯМОГО МАРКЕТИНГУ "МЕТА"

# ДИРЕКТ-МАРКЕТИНГ В ІНДУСТРІЇ БІЗНЕСУ

**Сьогодні директ-маркетинг у розвинених країнах є цілковито необхідним супутником будь-якого товару.**

**Бум у сфері директ-маркетингу підтверджується даними, що містяться у дослідженні, підготовленому для FEDMA (Federation of European Direct Marketing). З 1995 до 2000 року обсяг європейського ринку прямого маркетингу виріс на 11,6% і досяг у 2000 році суми 43,031 млрд євро. У Західній Європі він уже цілком пройшов стадію формування і на сьогоднішній день є високорозвиненою галуззю. Витрати на ДМ у середньому складають 51,8% сукупного рекламного бюджету.**

**У США, згідно з даними, озвученими на щорічній конференції Американської асоціації прямого маркетингу (DMA), оборот сектора ДМ становить 161,3 млрд дол. Це пов'язано з тим, що нині рекламодавці переорієнтовують свої маркетингові бюджети саме в цей сектор. За прогнозами DMA, щорічне зростання обороту в прямому маркетингу з 2004 до 2009 р. складе 6% у порівнянні з 2,4% у 1999-2004 р. У 2004 р. воно досягло 149,3 млрд дол., що становить 47,9% усіх рекламних бюджетів.**

**Курс директ-маркетингу є обов'язковою частиною програм усіх західних університетів. Існує навіть спеціалізований університет, працює безліч дослідницьких організацій.**

**За оцінками фахівців, у світі налічується понад 80 000 таких організацій. Ці цифри наведені без врахування періодичних видань, що випускаються не членами національних асоціацій. У світі видається понад 40 періодичних видань на тему директ-маркетингу.**

**Досить повно розроблена законодавча сфера. Склалися корпоративні правила для фахівців у цій галузі певне зведення писаних і неписаних норм, що ставлять свого роду етичні перешкоди для вторгнення у приватне життя клієнта.**

**Директ-маркетинг "спровокував" появу таких, зокрема, технологій, як комп'ютерна телефонна чи інтернет— поліграфія.**

**В цьому світі, як кажуть, усе зрозуміло. Набагато цікавіше розібратися в тому, що відбувається в Україні.**

**Є стійка тенденція майже дворазового щорічного зростання частки директ-маркетингу в рекламних бюджетах. У 2005 р. сума цих витрат орієнтовно становить не менше 50 млн дол. (частка непрямої реклами складає 268 млн дол.). Обсяг рекламного ринку України за 2005 р. склав 835 млн дол., а в 2006 р. він може досягти понад 1 млрд дол. Якщо справа піде і далі такими чи близькими темпами, то до 2010 р. ми цілком здатні зрівнятися з Європою в частині директ-маркетингу щодо витрат, пов'язаних із просуванням товару.**

*МвУ: — Як виглядає ринок прямого маркетингу в Україні сьогодні? Хто є оператором ринку, основними гравцями?*

На ринку більш-менш професійно працюють близько 40 операторів (сюди включаються і фірми, що надають послуги кур'єрської доставки рекламних матеріалів).

Спеціалізованих агенцій прямого маркетингу, що здатні розробити і надати весь комплекс дм-послуг налічується 10. В основному усі вони зосереджені в Києві. За останні 2-3 роки в Києві з'явилися 3 нових спеціалізованих Call-центри, кілька спеціалізованих мейлінгових центрів, фірм, що роблять послуги з використанням технологій мобільного зв'язку.

Фахівці вважають, що ринок ДМ є одним із таких, що найбільш динамічно розвиваються.

Серед основних факторів, що сприяють зростанню ринку ДМ, оператори називають законодавчо введені обмеження на рекламу тютюнових і алкогольних виробів.

Значний вплив на зростання ринку робить розвиток торгівлі за каталогами.

Варто відзначити і ряд проблем, що є на нашому ринку.

Один з них — нестача легальних баз даних, точніше дуже обмежені можливості їх оренди, особливо це стосується баз даних фізичних осіб. Не вистачає кваліфікованих кадрів, які б могли розробляти грамотні дм-кампанії і пояснювати клієнтам найпростіші прийоми підвищення їхньої ефективності. Це дуже серйозна проблема, яка не вирішується в Україні. Відсутні спеціалізовані програми одержання MBA з прямого маркетингу. Така програма дала б величезний поштовх розвитку ринку.

*МвУ: — Як регулюється ринок? Місце Закону "Про інформацію" в Україні і бізнес практики агенцій прямого маркетингу?*

У нинішній час держава не занадто втручається у сферу ДМ. Законодавчі норми, що обмежують цю діяльність і пов'язані з використанням персональних даних, установлені Конституцією (ст. 32) і Законом

"Про інформацію" (ст. 23). Згідно з цими документами, заборонено використовувати персональні дані (а до них відносимо адреси і телефони фізичних осіб) без згоди на те їхнього власника.

Щоб більш чітко окреслити правила використання подібного роду інформації, уже не перший рік розробляється й обговорюється спеціальний Закон "Про інформацію персонального характеру" (у Росії в першому читанні аналогічний закон був прийнятий наприкінці минулого року) (див. подробиці на www.dma.com.ua, новини за 30 листопада 2005р.).

Не можна сказати, що ці документи цілком влаштовують працюючих на ринку ДМ — операторів як у Росії, так і в нас. Уведення додаткових обмежень і підвищення відповідальності зробить цей ринок більш закритим, створить певні труднощі.

*МвУ: — Яка роль Української асоціації директ-маркетингу на цьому ринку. Основні проекти.*

УАДМ виступає з ініціативою не чекаючи прийняття Законів, що регулюють нашу роботу, зв'язану з розробкою і здійсненням прямих маркетингових комунікацій, розробити зведення правил, чи так званий Етичний кодекс, узявши за основу аналогічні документи FEDMA.

Основна місія УАДМ — всебічний розвиток ринку ДМ у нашій країні. Тому твердження такого документа — вкрай важливе питання для галузі, особливо в той час, коли тенденція зростання і збільшення обсягу ринку ДМ у загальних рекламних бюджетах дедалі більш очевидна.

У нашій галузі, на жаль, відсутні професійні стандарти якості роботи і їх прийняття є на даний момент дуже актуальним.

У своєму сегменті ринку ми повинні створити саморегулюючу систему (позитивний приклад — галузь маркетингових досліджень ринку) і створити її потрібно на зрозумілих принципах, на щирих і моральних засадах. Ці принципи повинні охоплювати в першу чергу наше ставлення і до прав людини, і до суспільства, і до наших клієнтів.

Багато в чому самим учасникам ринку потрібно дотримувати визначених принципів по відношенню один до одного. Усе це і пропонується описати в Етичному кодексі.

Крім того, нам необхідно займатися пропагандою професії та освітньою діяльністю в галузі ДМ в Україні.

Тут велику надію ми покладаємо на спільну роботу з УАМ і плануємо до 01.09.2006 р. запустити в життя навчальну програму підготовки кваліфікованих фахівців.

Перед нами стоїть завдання не тільки створити сприятливі умови для розширення ринку, але й брати участь у законодавчій практиці щодо ДМ. Адже наша участь багато в чому залежить від іміджу ринку ДМ в Україні, від іміджу компаній, що працюють у цій галузі.

Бажання УАДМ — зробити ринок ДМ по-справжньому цивілізованим.

Запрошуємо всіх професіоналів із усією серйозністю поставитися до нашої ініціативи і взяти активну участь у підготовці і здійсненні цього проекту.

*Розмову записав*
*Артем Андрусенко*

# FEDERATION OF EUROPEAN DIRECT MARKETING

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

# ЄВРОПЕЙСЬКА ФЕДЕРАЦІЯ ДИРЕКТ-МАРКЕТИНГУ

## ЄВРОПЕЙСЬКИЙ КОДЕКС ВИКОРИСТАННЯ ОСОБИСТОЇ ІНФОРМАЦІЇ У ДИРЕКТ-МАРКЕТИНГУ

### ПОЯСНЮВАЛЬНИЙ МЕМОРАНДУМ

ЄФДМ представляє сектор директ-маркетингу на європейському рівні. Її національними членами є асоціації директ-маркетингу 12 країн Європейського союзу (усі, крім Бельгії, Люксембургу та Данії), а також Швейцарія, Норвегія, Угорщина, Польща, Чеська та Словацька республіки, що представляють споживачів, постачальників послуг та медіа/носіїв директ-маркетингу. Членами ЄФДМ є також близько 350 компаній.

Представляючи прямо або через торгові асоціації в загальному близько 10 000 європейських фірм або асоціацій, що займаються директ-маркетингом, ЄФДМ є ідеальною організацією для розробки Кодексу щодо захисту інформації для організацій, які задіяні у цій сфері. Документ був підготовлений у ході дискусій з Article 29 Group. Цей необхідний інструмент є інтерпретацією Європейської директиви по захисту інформації. Він розроблений таким чином, щоб був зрозумілим для фахівців, які займаються директ-маркетингом. У деяких пунктах Євродирективи, де практика вже виходить за межі рівня, встановленого цим документом, або де ЄФДМ рекомендує, щоб так було, такі вищі стандарти практики включено.

Усі національні члени ЄФДМ, у тому числі торгові асоціації, погодились у своїх власних національних кодексах всіляко забезпечувати підтримку рівнів захисту інформації на такому високому рівні, який має Кодекс ЄФДМ, хоча у випадках, де

національне законодавство або власні установчі документи зобов'язують до цього або принаймні дозволяють, їх національний кодекс повинен мати навіть вищі стандарти.

Цей кодекс головним чином був розроблений як інструмент найкращої практики. Він призначений для використання як рекомендації в рамках відповідних законів. Прямі члени ЄФДМ діятимуть згідно зі стандартами, викладеними у Кодексі ЄФДМ, які є для них обов'язковими в рамках національного законодавства та власних регулятивних кодексів. Цей кодекс не має на меті зменшити або замінити можливість застосування національного законодавства та правил діяльності у даній сфері.

ЄФДМ сподівається, що вона активно пропагуватиме та розповсюджуватиме ідею того, що Кодекс ЄФДМ повинен застосовуватись усіма європейськими асоціаціями, що діють у сфері директ-маркетингу, незалежно від того, чи вони є членами федерації, чи ні, та використовуватимуть положення Кодексу як загальний стандарт у всьому, що стосується роботи в цій індустрії.

ЄФДМ також припускає можливість того, що цей Кодекс є лише першим етапом безперервного розвитку найефективніших норм у галузі захисту інформації. Подальші видання Кодексу будуть більш складними та продовжуватимуть відображати постійно зростаюче намагання відповідальних практиків цієї галузі бути найкращими. Подальші видання також відображатимуть усі зміни щодо цієї галузі, які відбуватимуться у європейському законодавстві. Також застосування правил індустрії в межах правління ЄФДМ буде підніматись до такого рівня, щоб постійно відповідати законним та постійно зростаючим сподіванням споживачів продуктів індустрії.

Потрібно також пам'ятати, що законодавство у сфері захисту інформації може бути застосоване при обробці особистої інформації з використанням будь-яких засобів.

Слід зазначити, які різні способи комунікації, що використовуються в директ-маркетингу, призвели до того, що були розроблені різні адміністративні положення та інструкції. Директиви 97/66/ЕС (Телекомунікації та конфіденційність) та 97/7/ЕС (Дистанційний продаж) вимагають узгодження усіх питань стосовно інформації ще до того, як комерційна комунікація розпочнеться та інформація про продукти і послуги буде відіслана до потенційних споживачів по факсу або ж через автоматичні системи розсилки інформації. Директива 2002/58/ЕС (Конфіденційність та електронна комунікація) також вимагає узгодження усіх питань до того, як почнуть використовуватись засоби комунікації (наприклад, електронну пошту) для зв'язку зі споживачами, які до того не мали жодних відносин зі збирачем інформації.

Цей Кодекс повинен читатись у доповненні з вже існуючими кодексами ЄФДМ і тими, що в майбутньому видаватимуться, включаючи Європейські принципи використання телефону бізнесом як засобу для здійснення маркетингових заходів. Також потрібно завжди враховувати Кодекс електронної комерції для суб'єктів європейського бізнесу (The Electronic Commerce Code of Conduct for European Business). Цей документ повинен застосовуватись у поєднанні з Глобальною конвенцією щодо телефонних послуг та послуг глобальної мережі Інтернет[1].

Кодекс розроблений для використання у процесі роботи з особистою інформацією, з якою мають справу директ-маркетологи з усього Європейського союзу та країн, що поки ще не увійшли до нього[2], проте які мають вже розроблені національні закони щодо захисту інформації, що не суперечать Директивам Європейського союзу.

**Усі положення цього Кодексу можуть бути застосовані без упереджень до положень застосовуваного національного законодавства. У тих випадках, де існують особливі вимоги на національному рівні, вони повинні відповідати усім правилам щодо законодавства, викладеним у цьому Кодексі, а також мають відповідати законодавству Європейського союзу.**

## ВИЗНАЧЕННЯ

### ДИРЕКТ-МАРКЕТИНГ

Розповсюдження будь-якими засобами (включаючи, проте не обмежуючи лише ними, — поштою, факсом, телефоном, послугами on-line) будь-якого рекламного або маркетингового матеріалу, що розроблені директ маркетологом, або під його керівництвом, і який спрямовується безпосередньо конкретному індивідіуму.

### ОСОБИСТА ІНФОРМАЦІЯ

Особиста інформація — це будь-яка інформація, яка пов'язана з ідентифікацією особи, або може бути використана для її ідентифікації. Особа, яку ідентифікують — це особа, яка може бути ідентифікована прямо або опосередковано, зокрема дані про ідентифікаційний код, або ж згадуються один чи більше факторів, що вказують на її особливості фізичного, фізіологічного, розумового, економічного, культурного або соціального характеру.

***Примітка***

Термін "особиста інформація" означає інформацію, яка має відношення до будь-якої особи, подається у такій формі, що особа ця може бути ідентифікована, зокрема може бути включене лише під прізвищем. Деяка інформація, що не містить прізвище особи, також вважається особистою і отже повинна подаватись згідно з правилами цього Кодексу. Це, наприклад, такі випадки, коли згадується поштова адреса або номер телефону,

[1] *Європейську конвенцію щодо телефонних послуг та Інтернету, Кодекс електронної комерції ЄФДМ, а також європейські принципи використання телефону як засобу здійснення маркетингових заходів підприємствами можна отримати у ЄФДМ. Детальна інформація також міститься на сайті http://www.e-mps.org. Список Robinson дорівнює Preferance Services (див. зноску)*

[2] *Країни Єдиного економічного простору (ЕЕА) та інші європейські країни, в яких закони щодо захисту особистої інформації готуються та впроваджуються на адекватному рівні.*

факсу, електронна адреса, посада, за допомогою яких встановлення особи є ймовірним.

**СЕНСИТИВНА ІНФОРМАЦІЯ**

Будь-які дані, що можуть розкрити наступну інформацію про особу, вважаються сенситивною інформацією та є об'єктом обмежень під час їхньої обробки:

- Расове та етнічне походження;
- Політичні погляди;
- Членство у профсоюзі;
- Релігійні або філософські переконання;
- Фізичний або емоційний стан (здоров'я);
- Сексуальне життя;
- Дисциплінарні порушення, судимості та дані служб безпеки.

**ДИРЕКТ-МАРКЕТОЛОГ**

Будь-яка фізична або юридична особа (включаючи представників доброчинних організацій та політичних партій), що розповсюджує будь-якими засобами, (включаючи, проте не обмежуючись, поштою, факсом, телефоном або засобами електронного зв'язку тощо), будь-яку інформацію рекламного характеру або маркетинговий матеріал, що спрямовується до конкретних осіб.

**ІНФОРМАЦІЙНИЙ СУБ'ЄКТ**

Індивідіум для якого персональні дані можуть бути ідентифікованими або за допомогою яких він може бути індентифікованим.

**КООРДИНАТОР З ЗАХИСТУ ІНФОРМАЦІЇ**

Будь-яка фізична особа, призначена оператором (контролером) інформації, що виконує функції, описані у цьому Кодексі.

**КОНТРОЛЕР ІНФОРМАЦІЇ**

Для будь-яких цілей цього Кодексу, термін "Контролер інформації" використовується для позначення будь-якої фізичної або юридичної особи, що визначає та контролює (самостійно або разом з іншими фізичними чи юридичними особами) цілі та шляхи, за допомогою яких відбувається або повинна відбуватись обробка особистої інформації.

***Примітка***

Контролера інформації не слід плутати з власником інформації. Наприклад, організація може бути власником інформації або бази даних (тому що та фізична або юридична особа володіє правами використовувати згадувану базу даних) і водночас може бути оброблювачем або контролером процесу обробки останньої. У той же час кваліфікацію та досвід контролера інформації та оператора інформації не слід ототожнювати. Оператор інформації — це не завжди та ж особа, що і Контролер.

**ОПЕРАТОР ІНФОРМАЦІЇ**

Будь-яка фізична чи юридична особа за винятком працівника служби контролю за інформацією, що обробляє особисту інформацію дотримуючись інструкцій, своїх обов'язків та вказівок Контролера інформації.

**ТРЕТЯ СТОРОНА**

Будь-яка фізична або юридична особа, яка не є інформаційним суб'єктом, контролером інформації або оператором інформації, жодним з агентів / співробітників відділу контролю за інформацією.

***Примітка***

Контролер інформації може призначати компанію А як їхнього оператора інформації. Оператор інформації може працювати з останньою лише дотримуючись інструкцій Контролера інформації. Однак, Контролер інформації вирішує питання стосовно найму компанії В, яка і стане Третьою стороною.

**РОБОТА З БАЗОЮ ДАНИХ**

У цьому Кодексі термін "обробка" вживається для позначення автоматизованих операцій, що виконуються із особистою інформацією для цілей директ-маркетингу. Неавтоматичні операції також покриваються цим Кодексом у тому випадку, якщо вони виконуються у структурований спосіб згідно з особливими критеріями, що дають можливість вільного доступу до інформації.

***Примітка***

Цей термін покриває кожний з окремих етапів операцій, що їх організація може здійснювати з особистою інформацією починаючи з етапу первинного збирання до знищення її, а також включаючи будь-які інші проміжні операції, такі як ректифікацію, збереження, захист та розголошення. Цей Кодекс застосовується лише для процесів, які пов'язані з директ-маркетинговою активністю. Маркетологи повинні також перевіряти, що інші типи операцій з базою даних, які вони проводять, також відповідають усім правилам, які стосуються захисту інформації.

**РОЗГОЛОШЕННЯ**

Будь-яка передача (постачання або роблення доступною) особистої інформації (наприклад, оренда, продаж) третім сторонам.

**ДІТИ**

Будь-які особи, що не досягли 14-річного віку, якщо інше не визначене національним законодавством/ власними правилами.

**БАТЬКИ**

Батьки дитини або законний опікун.

## 1. Законодавство

**1.1. Директ-маркетологи, що засновані на території Європейського союзу/ЕЕА (Єдиного європейського простору)**

Коли директ-маркетингові агенції засновують на території Європейського союзу/ЕЕА, вони повинні знати норми національного законодавства якого вони повинні дотримуватись, та вони повинні зважати на наступні правила:

1.1.1. Якщо Директ-маркетолог має лише одну установу на території Європейського союзу/Єдиного економічного простору і, таким чином, має лише одного Контролера інформації, то до нього застосовується закон території де він заснован, а також правила, викладені у пункті 1.1.4.

1.1.2. У випадку, якщо організація має декілька установ на території Європейського союзу/Єдиного економічного простору, і лише одна з цих установ є такою, що має статус Контролера інформації, коли інші ус-

танови є операторами, вона повинна поважати національні закони Контролера інформації, виняток можуть становити лише випадки, коли оператору необхідно дотримуватись законодавства у тих випадках, коли йдеться про гарантування безпеки інформації.

1.1.3. Якщо організація, що займається директ-маркетингом, має декілька установ, розміщених у країнах-членах Європейського союзу/Єдиного економічного простору, і кожне з цих утворень діє як Контролер інформації, вони повинні діяти відповідно до чинного національного законодавства тієї країни, в якій така установа розміщена.

1.1.4. Якщо організація, що займається директ-маркетингом і діє як Контролер інформації, використовує послуги оператора інформації від агента, який розташований на території іншої країни, яка, однак, є членом ЄС/ЄЕП, то організація, що займається операцією з базою даних, повинна застосовувати законодавство тієї країни, в якій розташований Контролер інформації, виняток становлять лише заходи безпеки — у цьому випадку застосовується законодавство тієї країни, у якій знаходиться оператор.

1.1.5. Той факт, що інформація надходить від фізичних осіб з однієї або більше країн ЄС/ЄЕП, або ж з країн, що знаходяться за межами цієї території, не є вирішальним фактором у визначенні законодавства, яким потрібно керуватись.

### 1.2. Контролери інформації засновані не на території ЄС/ЄЕП

Коли Контролер інформації заснован не в країні-члені ЄС/ЄЕП, а в країні, яка не має адекватного рівня захисту, і коли такий Контролер інформації не застосовує будь-яких форм або механізмів для захисту інформації, які прийняті в ЄС/ЄЕП, якщо він використовує Оператора, чиє обладнання знаходиться в країні-члені ЄС, то він повинен керуватись законами однієї з країн-членів (де знаходиться обладнання — *прим. перекладача*) (наприклад, телефонний центр задля збору інформації, офісними приміщеннями, щоб обробляти особисту інформацію від їхнього імені тощо). У такому випадку:

1.2.1. Контролер інформації повинен визначити представника — (фізичну або юридичну особу), що є резидентом країни-члена ЄС/ЄЕП, у якій відбуваються операції. Такий представник відповідатиме перед уповноваженими органами місцевої влади, щоб гарантувати те, що під час його діяльності використовується законодавство відповідної країни. (Це, однак, не означає, що уповноважені органи виконавчої влади не можуть застосовувати відповідні санкції до самого Контролера).

1.2.2. Застосовується законодавство тієї країни, у якій знаходиться представник.

1.2.3. Дотримання пункту 1.2. не є обов'язковим, якщо обладнання використовується лише для транзиту у межах ЄС/ЄЕП (наприклад, якщо Контролер інформації знаходиться у Канаді, інформація збирається у країнах, які не є членами ЄС/ЄЕП, а потім надсилається через телекомунікаційні мережі Об'єднаного королівства назад у Канаду).

## 2. Отримання особистої інформації

### 2.1. Збір інформації безпосередньо від суб'єкту бази даних

У процесі збирання інформації Контролер інформації повинен гарантувати, що отримання останньої провадиться у чесний спосіб, а також те, що об'єкт інформації, як це зазначено у даному Кодексі, має право на дану ним інформацію, і згідно цього Кодексу вона захищена.

**Загальні принципи чесної обробки інформації**

- *Важлива інформація*

Контролери інформації повинні гарантувати, що Суб'єкт бази даних інформований про:

— особу Контролера інформації (наприклад, знають його ім'я, адресу);

Таблиця 1

**Різні можливі ситуації резюмовані, з практичних причин, подані в таблиці:**

| | ФАКТИ | | | | ЗАСТОС. ЗАКОНОДАВСТВО | |
|---|---|---|---|---|---|---|
| Випадки | Директ-маркетолог знаходиться у | Контролер інформації знаходиться у | Оператор знаходиться у | Інформація отримується від | По відношенню до оператора | По відношенню до заходів безпеки |
| 1-ий | BE | BE | BE | EU EEA US | BE | BE |
| 2-ий | BE NL UK | BE | NL UK | EU EEA US | BE | NL UK |
| 3-ій | BE | BE NL UK | FR | EU EEA US | BE UK NL | FR |
| 4-ий | BE | BE NL UK | SP PT LUX | EU EEA US | BE NL UK | SP PT LUX |

— мету (цілі) постачання інформації (наприклад, для трансакцій або з метою просування)

Така суттєва інформація повинна надаватись під час процесса збирання даних, якщо тільки вона не є повністю ясною з контексту (наприклад, якщо особа контролера, мета, з якою здійснюється дослідження, та назва компанії є чітко вказаними у листівці (проспекті)), або якщо суб'єкт бази даних вже має таку інформацію (наприклад, якщо він і компанія уклала договір).

- Інформація про право доступу до *даних* з метою коригування їх та заперечень з приводу останніх

Контролери інформації повинні гарантувати те, що суб'єкт бази даних проінформований про:

— їх право доступу до наданої ними інформації та виправлення помилкових даних, що їх стосуються;
— їх право на те, щоб до них не звертались з метою директ-маркетингу;
— їх право заборонити оператору використовувати її/його особисту інформацію для цілей директ-маркетингу.

**Розгляд особливих ситуацій**

- *Інформація щодо того випадку, якщо отримані дані будуть використані для заходів директ-маркетингу*

У випадках, коли контролер має намір використати інформацію для цілей директ-маркетингу, контролер інформації повинен гарантувати те, що суб'єкт бази даних повідомлений про такі наступні дії контролера, а також те, що він має право відмовитись від участі у такому проекті.

Обов'язком Контролера інформації є ознайомлення особи, що надає її, з усіма умовами на час збирання останньої, усі зусилля повинні докладатись для задоволення цієї вимоги. Проте у випадках, де це важко або ж неможливо здійснити (наприклад, маленькі рекламні оголошення або телемаркетинг) та дозволено національним законодавством, така інформація може надаватись відразу (настільки швидко, наскільки це можливо) після отримання даних від суб'єкта інформації, наприклад, тоді, коли суб'єкт інформації отримує первинну документацію (інвойс, чек тощо) у письмовій формі, або будь-якому медійному засобі.

- *Інформація стосовно розголошення*

На додаток до необхідної інформації у випадках, коли є намір передавання її третім сторонам, контролер інформації повинен гарантувати те, що особи, які надають інформацію, поінформовані про:

— будь-яких отримувачів або типів отримувачів її, і мету, з якою вона буде використана;
— їх право на заборону розголошення інформації для цілей директ-маркетингу.

Ця інформація повинна надаватись безпосередньо під час збирання даних, до цього повинні докладатись усі зусилля, проте у випадках, коли така умова є неможливою або важкою для виконання (наприклад, коли розміщуються невеликі за розміром оголошення або як засіб використовується телемаркетинг), і це не заборонено національним законодавством, особа, що надає інформацію, повинна завчасно отримати повідомлення про те, що остання передаватиметься третім сторонам.

Така інформація може не надаватись, якщо вона вже надійшла раніше у будь-який спосіб. Механізм передавання такої інформації повинен відповідати національному законодавству та має передаватись з виконанням юридичних вимог, що їх містить національне законодавство, яке застосовується.

- *Інформація, яку необхідно прийняти до уваги у разі використання анкет та інших форм опитування*

На додаток до цієї важливої інформації, контролери інформації повинні гарантувати те, що суб'єкти інформації проінформовані стосовно того, чи є відповіді на запитання анкети обов'язковими чи добровільними, а також про можливі наслідки того, що вони не дадуть відповіді на якесь із запитань (наприклад, включають такі ситуації, але не обмежуючись ними, неотримання подарунка у тому разі, якщо інформація буде отримана за допомогою анкет). Обов'язком Контролера є також простежити за тим, що не будуть задаватись зайві запитання.

Уся інформація стосовно питальників повинна надаватись під час процесу отримання інформації.

**2.2. Отримання інформації з інших джерел (не від суб'єкта інформації)**

2.2.1. У тих випадках, коли Контролери інформації не отримують її безпосередньо від суб'єктів інформації, вони зобов'язані вжити наступних кроків з метою гарантування того, що все ж суб'єкти інформації є обізнаними з усією інформацією, яку вони б отримали у разі прямого контакту з Контролерами інформації. Наприклад, списки, кампанії по збільшенню членства, або ж дані, отримані з анкет, повинні бути легітимними та відповідати принципам, викладеним у пункті 2.1.

2.2.2. Контролери інформації повинні надавати інформацію, про яку йдеться у пункті 2.1:

- на час отримання та запису інформації (обробки її);
- у випадках, коли намічається передача інформації Третій стороні не пізніше моменту розголошення інформації, якщо тільки суб'єкта інформації було про це заздалегідь попереджено.

2.2.3. За умови, якщо використовувана інформація була отримана з дотриманням усіх відповідних правил захисту даних, як випадок часткової відміни принципів, викладених у пункті 2.2.1., вище зазначена вимога не застосовується у особливих виняткових обставинах, де необхідними є неспіврозмірні зусилля для того, щоб представити таку інформацію, а також у випадках, коли вдаються до будь-яких запобіжних заходів, що є викладені у національному законодавстві. Це, зокрема, обставини, за яких виникають невідповідно великі часові або ж грошові витрати. Наприклад, коли інформація отримується від третьої сторони та має бути використана через короткий час, недоцільним буде негайне інформування про це суб'єкт інформації, коли можна за-

чекати до тих пір, поки не відбудеться контакт.

2.2.4. Ці фактори постійно необхідно буде збалансовувати з результатами, що матимуть місце для суб'єктів інформації внаслідок часткової відміни принципів пункту 2.2.1. Приклади таких обставин, коли може виникнути диспропорціональний ефект при незмінних інших обставинах, включають:

- бази особистих даних з метою блокування або здійснення перевірки та підтвердження адреси;
- де особиста інформація закрита аплікаційною формою Robinson List of Preference Service File;
- коли маркетолог частково знищує або обмежує особисту інформацію тих осіб з маркетингового списку, які не відповідають необхідному профілю.

2.2.5. Оцінивши всі релевантні фактори та прийнявши рішення щодо часткового послаблення принципів, викладених у пункті 2.2.1., контролери інформації повинні забезпечити підготовку відповідного документа, який би виправдовував прийняття такого рішення. У такому документі повинні бути викладені причини рішення, тип інформації, що її повинні будуть надати контролери інформації, а також пояснення того, чому суб'єкти інформації не зазнаватимуть упередженого ставлення до себе у разі застосування викладених вище дій з боку контролера інформації.

### 2.3. Збирання сенситивної інформації

Зважаючи на особливу важливість сенситивної інформації та беручи до уваги основні особисті права суб'єктів інформації, потрібно вживати особливі заходи при роботі з такою інформацією.

Якщо до особистої інформації, що збирається, входить також сенситивна інформація, то Контролер інформації повинен вимагати виключної згоди від суб'єкта інформації на отримання такої інформації та подальшу її обробку. Подібна згода повинна бути чіткою, даною добровільно та повідомленою у такий спосіб, щоб не залишалось сумнівів щодо неї. Виключна згода не обов'язково повинна бути викладена у письмовій формі, але надання письмової згоди є бажаним, оскільки створює надійне підґрунтя для доказів у майбутньому, не враховуючи наступних обставин:

- інформація була очевидно розголошена суб'єктом інформації (наприклад, у разі отримання інформації з якогось публічного джерела як довідник, де суб'єкт інформації мав вибір щодо того, чи надавати таку інформацію, чи ні) або;
- якщо інформація обробляється релевантною неприбутковою організацією, з політичною, філософською, профспілковою, релігійною метою. Якщо ж ці організації використовують такого роду інформацію без чіткої згоди суб'єкта інформації, вони повинні врахувати наступні обставини:

— роботу з інформацією потрібно проводити у рамках легітимних заходів, що ці організації проводять;
— мають бути запропоновані відповідні гарантійні заходи;
— операції повинні мати відношення лише до членів відповідних організацій або осіб, що регулярно контактують з ними;
— операція має відповідати цілям організацій, що не мають на меті отримання прибутку;
— інформація не може бути надана третім сторонам без згоди на це суб'єкта інформації.

Прикладом такого заходу може бути надсилання церковною або релігійною організацією листа до своїх членів, у якому оголошується публікація релігійного бюлетеня, на який усі зацікавлені можуть підписатись, або повідомляється збирання коштів для надання допомоги в особливій ситуації.

За жодних обставин компанії не можуть використовувати сенситивну інформацію у такий спосіб, що може порушити фундаментальні права або свободи суб'єкта інформації. Робота з останньою завжди повинна проводитись у рамках легітимних заходів.

У тих випадках, коли сенситивна інформація, отримана для заходів з директ-маркетингу, використовується в подальшому для статистичного аналізу, вона повинна надаватись в анонімній формі або хоча б бути переробленою у такий спосіб, щоб неможливо було ідентифікувати суб'єктів інформації, якщо лише Контролер Іформації не отримав виключної згоди на це від суб'єкта інформації.

### 2.4. Інші цілі

2.4.1. Якщо було прийняте рішення використати особисту інформацію для цілі, що є іншою, аніж та, задля якої вона збиралась спочатку, то Контролер інформації повинен спершу перевірити, чи нова ціль є сумісною з тією, про яку спершу було повідомлено. Якщо вона сумісна, то робота з інформацією з такою новою ціллю дозволяється. У випадку ж, якщо нова ціль не є сумісною із зазначеною під час збирання інформації, та подальша обробка даних може бути дозволена лише у тому разі, якщо вона проводиться з дотриманням чинного законодавства про захист даних.

2.4.2. При визначенні сумісності нової цілі Контролери інформації серед інших аспектів також повинні брати до уваги наступні критерії: чи нова ціль (цілі) суттєво відрізняється від тих, з якими ця інформація збиралась, чи суб'єкти інформації реально могли передбачити виникнення таких обставин, а також можливість їхньої заборони таких дій організації, якби вони про них знали. Контролер інформації повинен завжди враховувати національні аспекти щодо обробки інформації, які розробляються відповідним національним уповноваженим органом.

### 2.5. Власна розсилка

Контролер інформації для Власної розсилки повинен бути чітко визначений.

Власна розсилка — це коли Контролер інформації використовує дані третіх сторін у своїх поштових розсилках.

### 2.6. Спеціальні вимоги для дітей

2.6.1. При формуванні "Дитячої бази даних" Контролери інформації

повинні завжди вдаватися до всіх можливих заходів для забезпечення того, що дитина та/або один з батьків є належним чином повідомлені про цілі обробки інформації, що була отримана про дитину.

Зокрема. коли комерційні матеріали будуть направлятися дітям або, з іншого боку, буде збиратися інформація від дітей, — про це повинна робитись інформаційна примітка, що є доступною та повністю зрозумілою дітям.

2.6.2. У всіх випадках, коли застосовуване національне або європейське законодавство щодо обробки інформації вимагає згоду того, хто надає дані на їх обробку, Контролери інформації повинні отримати попередню згоду від хоча б одного з батьків Дитини. Форма та метод, за яких такий дозвіл має бути отриманий, повинні завжди бути узгоджені з відповідними законами, та саморегулюючими актами.

2.6.3. Контролери інформації повинні надавати одному з батьків дитини тих самих прав на отриману інформацію, як ті, що описані у пункті 3.5 цього Кодексу. Контролери інформації мають докладати всіх зусиль для перевірки та підтвердження того, що особа, яка користується правами дитини, є дійсно одним з батьків останньої.

2.6.4. Контролери інформації не повинні здобувати інформацію від дітей у формі гри, в якій за сприяння надаються призи, а також у будь-якій іншій формі, за якою криється отримання вигод для дитини у тому разі, якщо він (вона) надасть більше особистої інформації, ніж це потрібно для участі у такому заході.

## 3. Обов'язки Контролера інформації

### 3.1. Принципи захисту інформації

3.1.1. Контролери інформації повинні діяти згідно з наступними принципами: Особиста інформація повинна бути:

- оброблена неупереджено на законних началах, на легітимній основі (у відповідності із застосовуваним законодавством та умовами цього Кодексу);
- зібрана для визначених ясних та легітимних цілей (наприклад, для цілей, що проголошені перед місцевими органами влади, що займаються питаннями захисту інформації, — такі як торгівля на основі особистої інформації, продаж на відстані);
- використана лише для тих цілей[3], з якими вона отримувалась. Подальша робота не повинна проводитись, якщо вона суперечить викладеним вище цілям, якщо тільки суб'єкт інформації не дав свого виключного дозволу на такі дії;
- адекватною, релевантною (наприклад, нормальним для авіакомпанії буде те, що вона цікавиться у пасажирів їх звичками щодо харчування, які стосуються їхніх уподобань в їжі для того, щоб подавати на борту саме ті продукти, проте компанія по виробництву автомобілів не буде цікавитись у своїх клієнтів їх уподобаннями, що стосуються їжі, тому що вона не задовольняє попит клієнтів у продуктах харчування) та не виходити за межі цілей, задля яких вона була зібрана та /або у подальшому оброблена;
- точною та своєчасною. Цього можна досягти шляхом використання конфіденційних листів (зокрема General Robinson Lists[4]), публічно доступних даних та права поправок, що здійснюються суб'єктом інформації.
- дотримана у такій формі, що дає змогу ідентифікувати суб'єктів інформації лише в такій мірі, що є необхідною для цілей, з якими проводилось збирання інформації та для цілей, з якими вона використовуватиметься.

3.1.2. Контролерам необхідно мати контракт з оператором, що погоджується діяти згідно з відповідними принципами та інструкціями Контролера. Відповідальність за чесну та законну обробку стосовно суб'єкта інформації несе Контролер та вона не може бути передана оператору через складання договору чи контракту.

### 3.2. Реєстрація у відповідних органах виконавчої влади, що займаються захистом інформації

Контролери інформації повинні забезпечувати реєстрацію всіх операцій з обробки інформації відповідно до чинного законодавства.

### 3.3. Заходи щодо захисту інформації

3.3.1. Контролери повинні гарантувати, що їх працівники вживають всіх необхідних заходів для забезпечення належної безпеки інформації, беручи до уваги витрати на це та рівень майстерності щодо їх технологічного впровадження, а також сенситивність інформації, з тим, щоб запобігти випадковому та протизаконному знищенню даних або їх випадкової втрати, зміни та несанкціонованого розголошення даних або доступу до файлів з особистою інформацією. Для уникнення таких небажаних дій з інформацією в майбутньому, Контролери повинні вживати відповідних специфічних заходів, таких як Технології підсилення конфіденційності (ТПК). Письмова конвенція між тими, що надають списки в оредну, та тими, що оперують ними має гарантувати, що списки будуть використані відповідно та на основі принципів безпеки.

3.3.2. Такі заходи також включають забезпечення охорони будівель, в яких зберігається особиста інформація та/або обробляється, (включаючи доступ до будівлі), список уповноважених осіб (із зазначенням їхньої відповідальності) за доступ до даних, належні механізми індентифікації (наприклад, контроль за допомогою паролю), до зазначених вище заходів також відносимо безпеку передавання інформації між Контролером інформації та оператором.

[3] Див. приклад наведений в пункті 2.4.1. вище.

[4] Robinson lists дорівнює Preferance Services.

3.3.3. Контролери можуть звертатись до своїх Національних асоціацій з директ-маркетингу за рекомендаціями з приводу прийняття відповідних заходів безпеки та відповідних технологій.

3.3.4. Контролери повинні також впевнюватись у тому, що всі особи, які наймаються ними для роботи з інформацією, повинні також вживати відповідних заходів безпеки (включаючи повагу до конфіденційності), про що має згадуватись у контракті, про який йдеться у статті 3.3.1.

### 3.4. Точка контакту

3.4.1. Контролери повинні призначати Координатора з захисту інформації всередині організації, який був би контактною особою з відповідних питань щодо захисту інформації.

3.4.2. Функції координатора з захисту інформації повинні принаймні включати:

- моніторинг, що здійснюється самостійно або за допомогою когось іншого у відповідності з практикою організації у сфері захисту інформації із застосуванням законів та положень цього Кодексу;
- діяльність як контактної особи з відповідними органами виконавчої влади у сфері захисту інформації.

3.4.3. Національні асоціації з директ-маркетингу можуть забажати отримати імена координаторів із захисту інформації своїх членів для того, щоб передати цю інформацію відповідним органам виконавчої влади по роботі із захисту інформації.

### 3.5. Використання суб'єктами інформації своїх прав

У доповнення до того, що Контролери повинні погоджувати свої дії з принципами, викладеними у пункті 3.1., вони також мають рахуватись з усіма правами, що їх має суб'єкт інформації, та які визначаються цим Кодексом та відповідним законодавством, включаючи право на:

- заперечення оперування її або його інформацією для цілей директ-маркетингу, включаючи можливість того, що з ними контактуватимуть від імені когось іншого. Утримування даних з метою блокування комунікацій директ-маркетингу не буде вважатись використання інформації для цілей директ-маркетингу;
- заперечення розголошення інформації Третім сторонам, за винятком випадків, коли таке розголошення інформації вимагається національним законодавством;
- доступ та внесення поправок для уточнення даних відповідно до пунктів 4.1. та 4.2. цього Кодексу;
- вимогу знищення або блокування інформації, якщо оперування нею не відповідає нормам чинного законодавства;
- заборону на легітимних засадах оперування інформацією для цілей, що є іншими, ніж цілі директ-маркетингу, якщо інше не обумовлено у чинному законодавстві.

### 3.6. Розголошення списків

3.6.1. Контролери інформації, які розголошують свої списки іншим організаціям, повинні вдаватись до поміркованих кроків (скажімо вимагати приклад матеріалу), з метою розслідування намірів використання даних (наприклад, чи зміст інформації може бути нелегальним, неетичним або таким, що може зашкодити іміджу директ-маркетингу взагалі, або ж містити дані, що є неприйнятними, такі як порнографія).

3.6.2. Контролери інформації (наприклад список брокерів) повинні також мати договір, здійснений в письмовому вигляді укладений з потенційним користувачем (Третьою стороною), за яким останній зобов'язується діяти відповідно до принципів цього Кодексу перед тим, як розголошувати інформацію.

## 4 Поводження з вимогами суб'єкта інформації

### 4.1. Доступ до інформації

4.1.1. Кожен суб'єкт інформації має право отримати від контролера:

- підтвердження того, чи дані, що мають до нього/неї відношення, задіяні, а також інформацію, яка стосується принаймні цілей використання даних, категорій інформації, що використовується, а також інформацію про отримувачів або категорії отримувачів, яким ця інформація надається;
- комунікація з ним /нею у чіткій формі з приводу поточного процесу у базі даних, та будь-якої доступної інформації щодо їх джерела;
- інформацію щодо логіки, яка застосовується при будь-якій автоматичній обробці у випадку автоматизованих рішень[5].

4.1.2. Контролери, які отримують вимоги у письмовій або будь-якій іншій формі від суб'єктів інформації на перегляд своєї особистої інформації, повинні:

- ідентифікувати будь-яку спеціальну інформацію, яка може бути вимагатися суб'єктом в особливості, якщо вона стосується ідентифікації суб'єкта, з метою гарантувати, що суб'єкт інформації належним чином назван, має право переглянути свою особисту інформцію у тому числі де знаходиться запис (наприклад, кампанія по розсилці листів);
- надавати особисту інформацію у доступній та ясній формі, включаючи будь-які нотатки або роз'яснення усієї двозначної інформації — наприклад, список правил, що застосовувались Контролером інформації;
- повідомляти їх про будь-яку розумну плату, яку вони мають намір давати за надання інформації, якщо це дозволено національним законодавством; така винагорода не може перевищувати певний ліміт, що встановлюється національними інструкціями;
- повідомляти їх про будь-які алгоритми, що були використані в автоматизованих індивідуальних рішеннях[6] стосовно його/її даних

[5] Автоматизоване індивідуальне рішення — це будь-яке рішення, що має правовий ефект на суб'єкта інформації або суттєво впливає на нього/неї і яке базується лише на автоматизованому процесі з метою оцінці його або її як, наприклад, даних про кредитоспроможність. Автоматизована обробка індивідуальних рішень може використовуватись лише у відповідності до чинного законодавства.

з метою оцінки будь-яких питань, що стосуються суб'єкта інформації, наприклад, його кредитоспроможності.

4.1.3. Контролери не зобов'язані задовольняти всі запити, що надходять через великий термін часу (як це визначено у національному законодавстві та/або кодексі, що забезпечує заходи, які більше спрямовані на захист даних).

### 4.2. Ректифікація

Контролери інформації повинні задовольняти будь-які вимоги, що надходять у письмовій або будь-якій іншій формі, та стосуються ректифікації особистої інформації. Якщо є підстави для сумнівів у легітимності вимоги у ректифікації, потрібно вимагати додаткових доказів перед тим, як приступити до останньої. Це, наприклад, може бути випадок, коли вимога надходить від неповнолітньої особи без схвалення одного з батьків або ж законного опікуна, або якщо Контролер інформації утримує інформацію, яка полягає у тому, що вимога на внесення змін не підтверджена. Наприклад, якщо суб'єкт інформації стверджує, що він/вона ніколи не замовляв продукт у даної компанії, а ця компанія має докази такої покупки.

Суттєві легітимні підстави також існують, коли є достатньо причин для того, щоб повірити в те, що вимога є надмірною. Таке може, наприклад, статись через те, що вона часто повторюється.

Якщо приймається рішення про те, що інформація не буде уточнюватись, суб'єкт інформації обов'язково повинен бути про це поінформований.

### 4.3. Джерело інформації

Коли Контролери отримують вимоги у письмовій або будь-якій іншій формі від суб'єктів інформації, в яких останні бажають дізнатись про джерело інформації, то контролери повинні (у тих випадках, де це є законним та коли таке джерело може бути ідентифіковане шляхом докладання поміркованих зусиль) передати цю інформацію тому, від кого надійшов запит. Якщо ж інформація була зібрана з різних джерел, Контролери повинні зберігати список тих джерел, з яких була отримана Особиста інформація.

### 4.4. Час на розгляд вимог від суб'єктів інформації

4.4.1. Контролери інформації повинні надавати інформацію, яка вимагається пунктами 4.1., 4.2. та 4.3. у короткий термін, який не повинен перевищувати той, що встановлюється національним законодавством.

4.4.2. ФЄДМ рекомендує, щоб Контролери надавали таку інформацію протягом 20 робочих днів, якщо тільки не виникли надзвичайні обставини.

## 5. Система, що обслуговує список Robinson (Preference Service Systems)

### 5.1. Внутрішні закриті списки

5.1.1. Контролери інформації повинні гарантувати те, що система приховання інформації, яка використовується для блокування імен або інших важливих ідентифікаційних деталей, — наприклад, телефонні номери або електронні адреси (див. визначення особистої інформації суб'єктів інформації, які забажали, щоб до них не звертались з питань директ-маркетингу), діє у їхній базі даних.

5.1.2. У випадку, якщо контролери інформації отримають вимогу від суб'єкта інформації про те, що він не бажає, щоб до нього звертались з будь-яких питань, вони повинні як тільки це стане можливим, хоча б не пізніше 4 тижнів після отримання такої вимоги заблокувати ім'я такого суб'єкта інформації у їхній базі даних.

5.1.3. Контролери інформації, які відповідають на заявку суб'єкта інформації щодо того, щоб його/її "не турбували", повинні пояснити, що такі процедури можуть не відноситись до матеріалу з директ-маркетингу, що був підготовлений ще до того, як було отримано таку заявку. Контролери інформації повинні вживати всіх заходів для того, щоб гарантувати, що суб'єкт інформації більше не отримуватиме матеріалів, які стосуються директ-маркетингу, як тільки з'явиться така можливість та принаймні не пізніше 3 місяців після отримання запиту.

### 5.2. Preference Service Systems

5.2.1. Контролери інформації повинні діяти відповідно до принципів національних Preference Services[7], у тих випадках, де дія їх розповсюджується, та у випадку використання особистої інформації з інших країн, в яких такі послуги діють, регулярно очищувати свої списки відповідно до Preference Services, відповідно до світових Конвенцій з Preference Services. Директ-маркетингові асоціації, що працюють з Preference Services, повинні регулярно очищати свої файли.

5.2.2. Вимоги щодо приховання певних даних зберігаються у системі, що обслуговує список Robinson (Preference Service Systems) протягом принаймні трьох років або протягом терміну, що встановлений національним законодавством. В особливих випадках, одним з яких є електронна пошта. що обслуговує список Robinson, файли можуть коригуватись у період, що є меншим 3 років відповідно до національного законодавства з електронною поштою. що обслуговує список Robinson.

Поновлений архів вимог щодо приховування інформації повинен зберігатись протягом періоду, що мінімально становить три роки, або довше, якщо цього вимагає націо-

[6] Див. зноску 5.

[7] Ця система. що обслуговує список Robinson (Preference Services) може включати листи (список Robinson ), реєстрація по телефону (Telephone Preference), факсимільне повідомлення (Fax Preference) або повідомлення електронною поштою (E-mail Preference). Примітка, однак, Контролер повинен також в міру необхідності зважати на повідомлення автовідповідачів і факсів згідно з Директиви 97/66/EC (Telecomunication and Data Privacy Directive), точно також зважати на отримані електронні повідомлення згідно з Директивою 2002/58/EC (Directive on Privacy and e-Communication).

нальне законодавство з preference services. У особливому випадку, яким є електронне звернення, що зареєстроване в цій системі (Preference Service Systems) від самої особи, для коригування даних, може застосовуватись короткий період у випадках, де це дозволено національним законодавством.

Власник або менеджер системи preference service повинен повідомляти суб'єкту інформації про часовий період, протягом якого така вимога є дійсною, — наприклад, коли суб'єкт інформації отримує підтвердження його/її вимоги.

## 6. Передача інформації до країн, що не є членами Європейського союзу

У випадку передачі інформації до країн, що не є членами Європейського союзу, тобто до тих, що вважаються такими, що не мають відповідного рівня захисту[8], контролер інформації може передавати Особисту інформацію лише з вжиттям дієвих захисних заходів та шляхом підписання контракту (це нерідко має бути схвалено на національному рівні), або шляхом забезпечення будь-яких інших форм чи механізмів, що схвалені в ЄС, якщо тільки суб'єкт інформації не дав свого недвозначного дозволу, або якщо така передача інформації є необхідною для виконання контракту між суб'єктом інформації та контролером, або для здійснення передконтрактних заходів, що чиняться у відповідь на запит суб'єкта інформації.

## 7. Моніторинг

### 7.1. Відповідальність національних асоціацій директ-маркетингу

Національні асоціації директ-маркетингу є відповідальними за чітке дотримання принципів, викладених у цьому Кодексі, а також тих, що містяться в їх національних кодексах, та повинні вживати тих самих санкцій, що передбачені у їхніх країнах у разі порушення національних кодексів.

Компанії повинні постійно проводити моніторинг того, наскільки їх дії відповідають принципам, викладеним у цьому Кодексі (наприклад, через внутрішній аудит)[9].

### 7.2. Розгляд скарг

7.2.1. Національні директ-маркетингові асоціації повинні встановити процедуру, відповідно до якої вирішуватимуться всі скарги, що можуть виникнути внаслідок використання цього Кодексу на національному рівні.

7.2.2. Національні директ-маркетингові асоціації повинні призначати працівника всередині організації, яка буде нести відповідальність за розгляд скарг та діяти як контактна особа для ФЄДМ. Ім'я такого співробітника повинно бути повідомлено відповідному органу, що займається захистом інформації.

7.2.3. У разі, якщо національна асоціація з директ-маркетингу виявиться неспроможною вирішити скаргу, що надійшла від суб'єкта інформації, через те, що суб'єкти таких відносин знаходяться у різних країнах, про такі випадки необхідно повідомляти ФЄДМ, котра в свою чергу, повинна призначити працівника в асоціації, який відповідає за вирішення таких спорів.

7.2.4. Національні директ-маркетингові асоціації повинні якомога більше співпрацювати з органами місцевої влади, що займаються питаннями захисту інформації.

7.2.5. ФЄДМ також співпрацюватиме з іншими організаціями, що мають до цього відношення, а також з іншими урядовими організаціями.

### 7.3. Порушення принципів

7.3.1. Про будь-яке порушення цього Кодексу членами ФЄДМ буде повідомлено Комітету ФЄДМ, який зобов'язується його розглянути. Комітет із захисту інформації, враховуючи тип порушення, може прийняти рішення щодо надання рекомендації Раді ФЄДМ про виключення такого члена або інші санкції відповідно до своїх правил.

7.3.2. ФЄДМ може також вдатися до відповідних дій проти члена або суб'єкта, що не є членом ФЄДМ, з метою охорони етики професії[10].

7.3.3. Будь-які дії, що не відповідають принципам цього Кодексу, можуть також призвести до юридичних санкцій, які накладатимуться національними наглядовими органами.

### 7.4. Комітет із захисту інформації

7.4.1. Комітет із захисту інформації створюється у ФЄДМ з метою моніторингу того, наскільки виконуються принципи даного Кодексу. Комітет із захисту інформації звітує перед Радою ФЄДМ.

7.4.2. Комітет із захисту інформації складається з контактних осіб національних асоціацій з директ-маркетингу, як встановлено пунктом 7.2.2.; с кандидатом від FEDMA; а також трьох представників з компаній, що входять до складу Ради ФЄДМ.

7.4.3. Функції Комітету захисту інформації:

- виносити щорічно рішення щодо того, чи є доцільним внесення змін до Кодексу;
- подавати Article 29 Working Party разом з щорічним звітом щодо функціонування принципів Кодексу на національному рівні, а також при здійсненні заходів закордоном;
- вирішення скарг, що надходять з інших країн, разом з Міжнародною федерацією асоціацій директ-маркетингу та Союзу європейських стандартів реклами;
- розгляд будь-яких порушень цього Кодексу.

7.4.4. Комітет із захисту інформації повинен також розробляти внутрішні правила та процедури.

[8] Має використовуватись перелік країн, які мають адекватну систему захисту та застосовують процедури, визначені Європейською колегією.

[9] Повинні вважатися по перевірці списків виборців Національними Державними органами влади.

[10] Наприклад, бельгійські професійні організації можуть вживати заходів на цих підставах.