ЕТИЧЕН КОДЕКС ЗА ПОВЕДЕНИЕ НА АДМИНИСТРАТОРИТЕ НА ЛИЧНИ ДАННИ

ВЪВЕДЕНИЕ

На 27.12.2005 г. влезе в сила Закон за изменение и допълнение на Закона за защита на личните данни. Съгласно чл. 10, ал. 4 във връзка с § 52 от Преходните и заключителни разпоредби на закона Комисията за защита на личните данни следва в 3-месечен срок от влизането му в сила да приеме Етичен кодекс за поведение на администраторите на лични данни.

Разработването на кодекси за поведение има за цел правилното прилагане на националните разпоредби, съгласно чл.27 от Директива 95/46 на Европейския съюз /ЕС/. С договор, подписан в Амстердам, считано от 1 януари 1999 г. се създава нов член 286 в Договора за създаване на Европейската общност /ЕО/, съгласно който институциите и органите на ЕО следва да прилагат правилата на общността за защита на личните данни. Още преди тази дата Съвета на ЕС създава по реда на чл. 251 от същия договор независим надзорен орган в общността, който да отговаря за точното и еднакво прилагане на правилата за защита на личните данни. Неговите правомощия са уредени в Регламент №45/2001 на Европейския парламент и Съвета на ЕС от 18 декември 2000 г. за защитата на лицата при обработване на лични данни от институциите и органите на ЕО и за свободното движение на такива данни.

ЦЕЛИ НА КОДЕКСА

1. Постигане на точно и еднакво прилагане на Закона за защита на личните данни от всички администратори на лични данни при отчитане на специфичните особености на тяхната дейност.

2. Създаване на баланс между интересите на лицата и интересите на администраторите на лични данни в рамките на закона за адекватни мерки за защита на личните данни.

АДМИНИСТРАТОР НА ЛИЧНИ ДАННИ

1. Администратор на лични данни е всяко физическо или юридическо лице, орган на държавна власт или на местно самоуправление, който обработва лични данни.

2. Видът на обработваните лични данни, целите и средствата за обработване се определят със закон или от администратора на лични данни.

РАЗДЕЛ ПЪРВИ

ОБЩИ ПРАВИЛА ЗА АДМИНИСТРАТОРИТЕ НА ЛИЧНИ ДАННИ

Член 1
Законосъобразност на обработването на лични данни

1. Администраторите обработват само законно събрани лични данни, необходими за установени от тях конкретни и законни цели.

2. Събирането на лични данни е законно в случаите, когато е задължение или право на администратора, уредено в нормативен акт.

3. Законна е тази цел, която не противоречи на Конституцията, международните договори, ратифицирани по конституционен ред, обнародвани и влезли в сила за Република България, както и на други закони и Закона за защита на личните данни.

4. Администраторът поддържа личните данни във форма, която позволява идентифициране на физическите лица за срок, не по-дълъг от необходимия за изпълнение на целите, за които личните данни се обработват.

5. Обхватът на обработваните лични данни следва да съответства на целите, за които те се обработват.

6. Използването на лични данни за исторически, статистически и научни цели се извършва след превръщането им в ***анонимни*** и уведомяване на Комисията за защита на личните данни.

7. В случаите, когато обработването на лични данни се извършва ***единствено*** за целите на журналистическа дейност, литературно или художествено изразяване, то е допустимо

само доколкото не нарушава правото на личен живот на физическото лице - субект на данни.

Член 2

Обработване на специални категории лични данни

1. Администраторът е длъжен да спазва генералния принцип за ***забрана на обработване на специални категории данни*** /чл. 5, ал. 1 от Закона за защита на личните данни/. Изключения се допускат само в случаите, предвидени в чл. 5, ал. 2 от закона.

2. Физическото лице следва да бъде информирано от администратора ***преди*** обработването на специални категории лични данни, с оглед изразяване от негова страна на свободно и недвусмислено ***изрично*** съгласие.

Член 3

Съгласие за обработване на лични данни

1. Съгласието на физическото лице трябва да бъде ***свободно изразен, конкретен и осъзнат акт*** за желанието му, относно обработване на отнасящи се за него лични данни.

2. Когато дава съгласието си, физическото лице трябва да е убедено, че неговите данни ще бъдат използвани ***изключително и само*** с оглед на целите, определени със закон или от администратора и посочени надлежно в документите за регистрацията му в Комисията за защита на личните данни.

3. В случаите, при които предоставянето на данни е задължение по закон, администраторът следва да информира лицето за последиците при евентуален отказ от негова страна.

Член 4

Право на възражение от страна на субекта на лични данни

1. Физическото лице има право по всяко време на обработване да поиска блокиране или унищожаване /изтриване/ на събрани за него лични данни, в случаите, когато оспорва тяхната точност или обработването им е незаконосъобразно.

2. Администраторът е длъжен да гарантира упражняване правото на лицето по т.1.

Член 5

Право на достъп на лицето до отнасящи се за него лични данни

1. физическите лица имат право на достъп до отнасящи се за тях лични данни, по всяко време на обработване, без забавяне, в законоустановения срок, безплатно и в предпочитаната от тях форма.

2. Достъпът до личните данни на физическо лице се разрешава за потвърждаване на целта на обработването им, информиране относно категориите лични данни, които се обработват за него, както и за категориите, получатели на които те могат да бъдат предоставени.

3. Администраторът е длъжен да осигури достъп на лицата и за актуализиране или коригиране на техните лични данни.

4. Администраторът е длъжен, при поискване от физическото лице, да го информира и за логиката на всеки автоматизиран процес, който е свързан с обработката на неговите лични данни.

5. В случай че откаже предоставянето на достъп до лични данни на физическото лице, администраторът е длъжен да мотивира отказа си.

Член 6

Задължение за уведомяване на трети лица

1. Администраторът е длъжен да уведоми третите лица, пред които личните данни са били вече разкрити, за всички извършени с данните корекции, блокиране или изтриване.

2. Изключение от задължението по предходната точка е допустимо в случаите, когато уведомяването е невъзможно или изисква прекомерно усилие.

Член 7

Информиране на субекта на лични данни от страна на администратора

1. В случаите, когато данните не са получени от физическото лице, администраторът, получил данните, е длъжен да го информира за 2
целите на обработване, за категориите предоставени данни и техния източник, за получателите, на които ще бъдат предоставени, както и за правото му на достъп до неговите лични данни.

2. Администраторът може да го информира и за правното основание за обработване на личните му данни, както и за срока на съхраняването им.

3. Когато предоставената информация по т. 1 е класифицирана, отпада задължението на администратора за информиране на лицето.

Член 8
Технически и организационни мерки за защита на личните данни

1. Предвид състоянието и разходите за реализация администраторът е длъжен да гарантира надеждност на обработването, като осигури технически и организационни мерки за защита на личните данни срещу:

а/ случайно или незаконно разрушаване;
б/ случайна загуба или промяна;
в/ незаконно разкриване или достъп;
г/ нерегламентирано изменение или разпространение, както и всички други незаконни форми на обработване;
д/ незаконно копиране, изнасяне и разпространяване;
е/ изтриване (унищожаване) преди изтичане на необходимия срок за съхранение, съответстващ на целите, за които те се обработват.

2. При обработване по електронен път се предприемат специални мерки за защита.

3. При ръчно обработване на лични данни следва да се предприемат надлежни мерки, за да се предотврати непозволен достъп или разкриване, промяна, унищожаване или случайна загуба.

4. При автоматизирано обработване на лични данни трябва да се вземат технически мерки за защита, чрез които:

А/ да не се разрешава:
а/ четене, възпроизвеждане, промяна или премахване на носителя на данни;
б/ несанкционирано въвеждане в паметта, както и несанкционирано разкриване, промяна или заличаване на съхранени лични данни;
в/ несанкционирано използване на системите за лични данни чрез средства за пренос на данни;
г/ използване на системата за обработване до други лични данни, освен тези, до които имат право на достъп.

Б/ да се извършва:

а/ запис на информацията кои лични данни са съобщени, кога и на кого;

б/ възможна следваща проверка, както и установяване кои лични данни са били обработени, кога и от кого;

в/ обработване на лични данни от името на администратора, само по начина, предписан от него;

г/ контрол по пренасяне на носителя или по време на съобщаване, така че данните да не могат да бъдат четени, копирани или изтривани без разрешение.

РАЗДЕЛ ВТОРИ

ПРЕПОРЪКИ ЗА ПОВЕДЕНИЕ НА АДМИНИСТРАТОРИТЕ ПРИ ОТЧИТАНЕ СПЕЦИФИЧНИЯ ХАРАКТЕР НА ТЯХНАТА ДЕЙНОСТ

Член 9

Органи на държавна власт

1. В съответствие с Европейския кодекс за добро поведение на администрацията, органите на държавна власт обработват лични данни при спазване принципа на лична неприкосновеност и ненамеса в личния живот на гражданите.

2. Служителите от държавната администрация, имащи качеството на "обработващ лични данни" по смисъла на Закона за защита на личните данни, не допускат обработване на лични данни за незаконни цели и предоставяне на такива данни на неоторизирани лица.

3. Държавните органи в рамките на своята компетентност предоставят достъп до обществена информация при спазване изискванията на Закона за достъп до обществена информация и Закона за защита на личните данни.

4. Органите на съдебната власт приемат Правила за професионална етика на съдебните служители, включващи изисквания за защита на личните данни на гражданите.

Член 10

Управление на човешки ресурси

1. Набирането на персонал от страна на търговци, по смисъла на Търговския закон се осъществява чрез доброволно получаване на лични данни от страна на лицата – кандидати за работа.

2. Администраторите на лични данни в областта на човешките ресурси нямат право да обработват лични данни, свързани с расов или етнически произход, религиозни, философски и политически убеждения, участие в политически партии и организации, както и свързани със здравето, сексуалния живот и човешкия геном, освен при условията на чл. 5, ал. 2 от Закона за защита на личните данни.

3. Съхраняването на лични данни на кандидати за работа е недопустимо след реализиране на целите, за които данните се обработват, освен ако друго не е предвидено в закон.

4. Сдруженията за управление на човешки ресурси могат да приемат специфични правила за поведение, които да не противоречат на действащото в страната законодателство и международните договори, ратифицирани по конституционен ред, обнародвани и влезли в сила за Република България.

Член 11
Директен маркетинг

1. Администратори, които събират лични данни за целите на директен маркетинг, следва да спазват принципа на лична неприкосновеност и ненамеса в личния живот на гражданите, като се въздържат от изпращане на непоискана търговска кореспонденция.

2. Осъществяването на комуникация с цел директен маркетинг без съгласие на физическите лица е недопустимо.

3. Препоръчва се на администраторите в областта на директния маркетинг да приемат браншови Правила за поведение във връзка със защитата на личните данни при осъществяване на тяхната дейност.

Член 12
Финансово-счетоводна дейност

1. Финансово-счетоводните регистри се съхраняват в срокове, съгласно Закона за държавния архивен фонд.

2. Администраторите, обработващи лични данни за целите на финансово-счетоводната дейност, могат да приемат браншови Правила за поведение за защита на лицата при обработване на личните им данни с цел точно и еднакво прилагане на действащото законодателство.

Член 13
Банково и застрахователно дело

1. В съответствие с действащото в страната законодателство и международните договори, ратифицирани по конституционен ред, обнародвани и влезли в сила за Република България, администраторите в областта на банковото и застрахователно дело обработват лични данни при спазване принципа на лична неприкосновеност и ненамеса в личния живот на гражданите.

2. Изключение от принципа по т. 1 се допуска при обработване на лични данни за борба срещу финансиране на тероризма и изпирането на пари, както и за целите на националната сигурност на страната.

3. При приемане на Вътрешни правила и Общи условия администраторите от този сектор осигуряват баланс на интересите по предходните т. 1 и т. 2, като не допускат прекомерно събиране на лични данни, надхвърлящи целите за тяхното обработване.

Член 14
Пенсионна, здравна и социално-осигурителна дейност

1. Прехвърлянето на лични данни от един администратор на друг в областта на пенсионното, здравно и социално осигуряване е недопустимо без съгласието на съответното физическо лице, освен ако не е уредено в закон.

2. Съхраняването на лични данни след изпълнение на целите, за които се обработват, се допуска само съгласно Закона за държавния архивен фонд.

Член 15
Обществен ред и частна охранителна дейност

1. За спазване на обществения ред и при осъществяване на частна охранителна дейност, изключения от императивните норми за обработване на лични данни от страна на администраторите се допускат в случаите, когато са уредени в закон.

2.Видеонаблюдение се допуска за спазване на законоустановения обществен ред, както и по реда на Закона за частната охранителна дейност.

Член 16
Частно разследване

1. Администраторите обработват лични данни за целите на частно разследване при спазване на конституционните принципи на лична неприкосновеност и ненамеса в личния живот на гражданите.

2. Изключения от принципите по т. 1 се допускат само за целите на наказателния процес при наличие на достатъчно доказателства за извършено престъпление или с превантивна цел срещу извършването му.

Член 17
Правни услуги

1. Лица, осъществяващи правни услуги, могат съхраняват лични данни до окончателното извършване на правната услуга, освен ако със закон не е предвиден по-дълъг срок.

2. Адвокатските и други сдружения в сферата на правните услуги приемат правила за професионална етика, имайки предвид специфичните особености за защита на личните данни при осъществяване на тяхната дейност.

Член 18
Управление на собственост

1. Жилищно-строителните кооперации (ЖСК) и управителите на етажна собственост обработват лични данни при спазване принципа на лична неприкосновеност и ненамеса в личния живот на гражданите.

2. Съхраняването на личните данни на членовете на ЖСК и на живущите в етажната собственост се използва само за целите на управление на собствеността, освен ако друго не е уредено в закон.

Член 19
Информационни, компютърни и комуникационни технологии

1. Обработване, съхраняване и използване на лични данни във връзка с осъществяване на електронна търговия се извършва при спазване на правото на личен живот на потребителите.

2. Предоставянето на лични данни на потребител – физическо лице, с оглед индивидуализиране на страните по договор, преди неговото сключване за осъществяване на електронна търговия, се извършва при изрично съгласие на потребителя – физическо лице.

3. Далекосъобщителните услуги се извършват при гарантиране на свободата и тайната на съобщенията и спазване изискванията на Закона за защита на личните данни и Закона за далекосъобщенията.

4. Допуска се правомерното записване на съобщения в процеса на законна търговска практика с цел доказване на търговски сделки, или на каквато и да е друга бизнес – комуникация, в съответствие с чл. 5 от Директива 2002/58/ЕО, като нова регулаторна рамка, действаща в държавите - членки на ЕС след 31 октомври 2003 г.

5. Операторите на далекосъобщителни услуги могат да обработват лични данни, необходими за разплащане, след предоставяне на услугата при формиране на абонатните сметки, както и за доказване на тяхната достоверност.

6. Съгласно Директива 2002/58/ЕО използването на непоискани съобщения чрез електронна поща за осъществяване на директен маркетинг, така нар.“спам”, е допустимо единствено с предварителното съгласие на абоната. Ако желае да получава спам, той има възможност да се включи в регистър за вписване, а ако не желае – в регистър за отписване, т.нар.“opt-in” и “opt-out” регистри.

Член 19
Образование

1. Обработването на лични данни в областта на образованието се извършва само за целите, за които са събрани.

2. След изпълнение на целите по т. 1 личните данни могат да се прехвърлят на друг администратор в случаите, уредени с нормативен акт, или се съхраняват по реда на Закона за държавния архивен фонд.

Член 20
Здравеопазване

1. Обработването на лични данни в областта на здравеопазването се извършва при спазване на Закона за защита на личните данни и Закона за здравето, като интересът за спасяване на живота и здравето на съответното физическо лице има приоритет.

2. В случаи на противоречие между Закона за защита на личните данни и Кодекса на професионалната етика се прилага Закона за защита на личните данни.

Член 21
Местно самоуправление

1. Органите на местно самоуправление, като задължени субекти по смисъла на Закона за достъп до обществена информация предоставят лични данни, когато те се отнасят за информация, свързана с обществения живот в Република България и дават възможност на гражданите да си съставят собствено мнение за тяхната дейност.

2. Личните данни, обработени от органите на местно самоуправление, за провеждане на местни избори, референдуми и други цели от обществен интерес се съхраняват след реализиране на целите само в случаи, предвидени със закон.

ЗАКЛЮЧЕНИЕ

Етичният кодекс не налага нови законови задължения за администраторите на лични данни. Той отразява главните принципи, които трябва да бъдат спазвани при обработване на лични данни, за да се гарантират неприкосновеността и защитата на лицата в тази област.

Отчитайки необходимостта от развитието на култура, в която личния живот, защитата на данните, сигурността и конфиденциалността на информацията, трябва да бъдат разглеждани и като задължителна норма на поведение, Комисията за защита на личните данни насърчава администраторите да създават етични кодекси, съобразени със спецификата на своята дейност, в съответствие с изложените в настоящия Кодекс правила.

Препоръчва се на браншовите организации да приемат етични кодекси на администраторите, съдържащи правила за поведението им в областта на защитата на личните данни.

За изпълнение на настоящия кодекс администраторите на лични данни си сътрудничат при прилагането му и при изготвяне на етични кодекси в своята област.

Администраторите на лични данни гарантират спазването на кодекса, като при нарушаването му могат да налагат дисциплинарни наказания по реда на Кодекса на труда и Закона за държавния служител.