

**Пловдивски Университет „Паисий Хилендарски‟**

# Факултет: “Математика и Информатика ”

***Избираема Дисциплина: Бизнес Право***

***Тема: 15. Лични данни и способи за защита***

**Изготвил: Александър Каранейчев**

**Фак. Номер: 2001261008**

**Специалност: Информатика**

Според българският закон, лични данни са всяка информация за физическо лице, която разкрива неговата физическа, психологическа, умствена, семейна, икономическа, културна или обществена идентичност. Значимостта и на правото на достъп до информация, и на защитата на личните данни, е установена с Конституцията на Република България. И двете права са конституционно гарантирани права на гражданите и съгласно чл. 57 от Конституцията са неотменими. Чл. 32 прогласява правото на всеки на неприкосновеност на неговия личен живот, а чл. 41 - правото на гражданите да търсят и получават информация.

***Права на гражданите по закона****:*

1.Гражданите имат право на защита срещу безцелно и незаконно събиране на данни за тях от държавата.

2.Гражданите имат право на защита срещу незаконно прехвърляне на данни за тях от една институция към друга.

3.Гражданите имат право да знаят кой, кога какви данни събира за тях и с какви цели.

4.Гражданите имат право на достъп до вече събраните данни, както и да искат поправянето или заличаването им в съответните случаи.

5. Гражданите имат право на специална защита на определени данни, разкриващи - расов или етнически произход, политическа или религиозна принадлежност, здраве, сексуален живот и обеждения.

Още 1993 г. в България започва да се говори за защита на личните данни и са подготвени законодателни текстове, свързани преди всичко с институционална рамка на тази защита. Проектът бива отхвърлен през 1996 г. отевропейски наблюдатели порадинесъответствието му с приетата

тогава **Директива 95/46/ЕС**.

**Като цяло нарастващия интерес към темата за защита на личните данни се дължи на развитието на информационните технологии, даващи възможност да се обработват бързо огромни бази с лична информация и засилващите се от това опасения за злоупотреба с тях.**

**Наред с това защитата се разглежда и като основно средство на гражданите да се предпазят от неправомерни действия на администрацията, някои стопански обекти или юридически лица. Като част от правото на неприкосновеност тя участва в различни сфери от живота ни и най-често във връзка с нея се нарушава баланса между личната неприкосновеност и други основни човешки права. Такива като правото на достъп до информация и свободата на словото.**

Ако погледнем по-широко на проблема - личните данни на хората никога не са били защитавани ефективно у нас. **Особено чувствителна е темата за защита на личните данни в България поради нестихващите скандали свързани нарушаване на личната неприкосновеност и използване на лични данни в борбите за политическа власт. Традициите и огромното наследство оставено от структурите на бившата Държавна сигурност за използване на лични данни за постигане на нетолкова чисти цели все още имат водещо място в силовите министерства въпреки твърденията за устояване на демократични принципи и спазване на правата на личността.**

**Не спират скандалите за неправомерно използване на специални разузнавателни средства и акции срещу водещи политици. Това са част от проблемите от политическият аспект на защитата на личните данни. От друга страна са злоупотребите ставащи с личните данни съхранявани по трудови договори, банкови сметки и др. При изнасяне на данни от съответното търговско дружество или организация стават възможни фалшификации, незаконни прехвърляния на имущество, присвояване на средства и т.н. Стига се до там, че дори и лица без никакво право изискват лични данни, като например при влизане в дадени учреждения или жилищни сгради се налага да се остави лична карта или да се дадат имена, адрес и единен граждански номер, в пълна противоположност на законовите разпоредби и нарушение на Закона за зашита на личните данни.**

Защитата на личните данни на всеки гражданин представлява важен елемент от упражняванетона правото на неприкосновеност на личността - едно от основните човешки права и свободи в демократичните общества.

От друга страна, демократичното управление и принципите на правовата държава изискват гражданите да са надлежно информирани за начина по който са на по-голям обществен интерес, и следователно тяхното право на неприкосновеност на личната сфера е по-ограничено. Данни, които пряко

засягат изпълнението на функциите на обществената длъжност, която лицата заемат, следва да бъдат обект на публично достояние и контрол.

**За да разясним  защитата на лични данни, какво определяме като лични данни и кои точно извършва тази защита ще разгледаме по-нататък основните принципи и разпоредби в Закона за зашита на личните данни и устройството на орагана, който я упражнява (Комисията за защита на личните данни). Също така ще разгледаме и с какво се занимава комисията и какви нарушения най-често отчита тя.**

**Като лични данни в България закона разбира всяка информация отнасяща се до физическото лице, което е идентифицирано или може да бъде идентифицирно пряко или непряко  чрез идентификационен номер или чрез един или повече специфични признаци.**

# *Принципи за правомерно обработване на лични данни*

Основните принципи, на които трябва да се основава правомерното обработване на лични данни на физическите лица /ФЛ/ от страна на администраторите на лични данни са посочени в ЗЗЛД. Съгласно чл. 2, ал. 2 от ЗЗЛД личните данни трябва:

- да се обработват законосъобразно и добросъвестно;

-да се събират за конкретни, точно определени и законни цели и да не се обработват допълнително по начин, несъвместим с тези цели; допълнително обработване на личните данни за исторически, статистически или научни цели е допустимо, при условие че администраторът осигури подходяща защита, като гарантира, че данните не се обработват за други цели;

-да бъдат съотносими, свързани със и ненадхвърлящи целите, за които се обработват;

-да бъдат точни и при необходимост да се актуализират;

-да се заличават или коригират, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;

- да се поддържат във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват; личните данни, които ще се съхраняват за по-дълъг период за исторически, статистически или научни цели, се поддържат във вид, непозволяващ идентифицирането на физическите лица.

**Нужно е да се изясни и какво точно представлява „обработка на личните данни”. Според формулировката в закона тя е всяко действие или съвкупност от действия, които могат да се извършат по отношение на личните данни с автоматични или други средства. Тук се включват събиране, записване, организиране, съхраняване, изменение, възстановяване, консултиране, употреба, заличаване или унищожаване и др. Реално погледнато почти няма юридическо лице, държавен орган или физическо лице – търговец или самоосигуряващо се лице, които да не използват в дейността си лични данни за физически лица . Особено широко тази сфера се застъпена в дейността на банките, телекомуникационните компании и др.**

**Държавата забранява обработката на лични данни разкриващи расов или етнически произход, политическа ориентация, религия, философски убеждения и др. Защитена от обработване информация също е членството в различни политически, религиозни, филосфски и синдикални формации, както сексуалния живот, здравето и човешкия геном.**

**Закона предвижда все пак обработка на тези данни, но при дадени условия. Такива са определени в областта на трудовите взаимоотношения или в случаите, когато физическото лице е дало изричното си съгласие за обработването им и това не противоречи на закона. При необходимост от защита на живота и здравето или решаване на проблеми  от естеството на националната сигурност също се допускат използване на личните данни, както и при положение, че лицето не е в състояние да даде съгласието си.**

**За да се ограничи произвола и злонамереното използване на събираните данни са въведени основни принципи за защита  на личните данни при тяхната обработка от различните администратори.Принцип на ограниченото събиране. Според него събирането на лични данни трябва да бъде в рамките на необходимото и информацията трябва да се набира по законен и обективен начин.**

**Принцип на ограниченото използване, разкриване и съхранение. Смисъла на този принцип е, че личните данни не трябва да се използват или разкриват за различни цели от тези заради, които са били събирани Личните данни трябва да бъдат съхранявани само толкова време, колкото е необходимо за изпълнението на тези цели.**

**Принцип на прецизността се изразява в това, да се изисква прецизност, пълност и актуалност, доколкото това е нужно за постигането на поставените цели.Принцип на сигурността и опазването – личните данни трябва да бъдат защитени с мерки отговарящи на чувствителността на информацията.Принцип на прозрачността. Органите на държавното управление трябва да осигуряват информация за политиките и практиките свързани с управлението на личните данни.**

**Принцип за достъп до собствени данни. Гражданите трябва да имат възможността да проверяват точността и пълнотата на личните данни и да ги поправят ако е необходимо. Чрез упражняването на този принцип гражданите осъществяват контрол върху дейността на администраторите. Особен случай тук е Закона за класифицираната информация, според който дадена информация може да се квалифицира като държавна или служебна тайна и по този начин достъпа до нея да бъде забранен, дори и когато тази информация касае само лични данни на дадено лице.**

**Тук остава въпроса дали дръжавата не оставя твърде широки правомощия на органтие си да отказват достъп до информация, като я определят като секретна.**

**След като основните принципи за защита на личните данни са изяснени е нужно да се разгледа и органа отговарящ за тази дейност. По-точно това е Комисията за защита на личните данни.** През 1998 България подписа **Конвенция № 108 на Съвета на Европа за защита на персоналната информация**. Не бяха създадени обаче необходимите закони, за да може да се ратифицира. В годишния доклад на Европейската комисия за 1998 г. се отчита, че са предприети първоначални стъпки за въвеждането на концепцията за защита на информацията.

Темпото на хармонизиране с европейското законодателство в България като цяло бива ускорено, но според Комисията са нужни още усилия по отношение на практическото му прилагане. През 1999 година се приемат закони, които да отговорят на изискванията на **Конвенцията 108 на Съвета на Европа за защита на личните данни** - **Закон за документите за самоличност (април 1999 г.); Закон за гражданската регистрация (юли 1999 г.). Националният план “Партньорство за присъединяване”,** стъпки в областта започват да се предприемат след 1997 г. Изискванията по отношение на защитата на личните данни, които България следва да изпълни, са вписани в Становището на Европейската комисия относно молбата на Република България за членство в Европейския съюз/ юли 1997/.

През 2000 година е създадена междуведомствена работна група за изготвяне на проектозакон за защита на личните данни. През месец декември 2001 г. Законът за защита на личните данни е приет от Народното събрания. Законът има за цел хармонизиране на българското законодателство в тази област с достиженията на правото на ЕС. **В тази връкза Закона за защита на личните данни се основава на принципите приети в европейското законодателство, с което се стреми да се постигне еднакво ниво на защита на информационните потоци с лични данни в съюза. Освен ангажимента на институциите стои и въпроса за това доколко са осведомени гражданите за техните права и доколко те самите следят за спазването им.**

**Дотолкова сме свикнали с всекидневната употреба на нашите лични данни, че рядко обръщаме внимание когато те са взимани с повод и без повод, законно или не. Незнанието и процедурната мудност развързват ръцете на администраторите и развихрят техния произвол.**

**Закона за защита на личните данни** предвижда, също така създаването на независим орган за наблюдение.През май 2002 година, пет години след подписването й, България ратифицира със закон на Народното събрание **Конвенция № 108 на Съвета на Европа за защита на лицата при автоматизираната обработка на лични данни**. Същия месец е създадена **Комисията за защита на личните данни (КЗЛД),** като независим колегиален държавен орган, който осъществява контрола по спазването на закона.

***ЕВРОПЕЙСКА ПРАВНА РАМКА В ОБЛАСТТА НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ***

Конвенция за защита на човешките права и основни свободи, подписана в Рим на 4 ноември 1950 г. с 11 протокола (позната и като “Европейска конвенция за правата на човека” и “ЕКПЧ”)

• Конвенция за прилагане на споразумението от Шенген от 14 юни 1985 година между правителствата на държавите от Икономическия съюз Бенелюкс, Федерална република Германия и Френската република за постепенното премахване на контрола по техните общи граници, Глава ІІІ., чл. 102-118

• Конвенция № 108 на Съвета на Европа от 28 януари 1981 г. за защита на лицата при автоматизираната обработка на лични данни

• Допълнителния протокол към Конвенцията за защита на лицата при автоматизирана обработка на лични данни, по отношение на надзорните органи и трансграничните информационни потоци от 08 ноември 2001 г. – Ратифициран със закон, обнародван в ДВ. бр. 6 от 22 януари 2010г.

• Препоръка No. R (87) 15 на Съвета на Европа Комитет на Министрите от 17 септември 1987 г. относно регулирането на използването на лични данни в полицейския сектор

• Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита за физическите лица при обработването на лични данни и за свободното движение на тези данни

 • Въз основа на Заключенията, след получаване на положителното становище на Европейския парламент, на 29 юни 2010г. Съветът прие Решение относно прилагането на разпоредбите на достиженията на правото от Шенген, свързани с ШИС. Съгласно документа от 29 юни 2010г. България може да зарежда данни в ШИС, а от 15 октомври 2010г. ще може да обменя реални данни в ШИС с държавите членки на шенгенското пространство.

• Регламент (ЕО) № 1987/2006 на Европейския парламент и на Съвета от 20 декември 2006 година за създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II)

• Решение 2007/533/ПВР на Съвета от 12 юни 2007 година относно създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II)

***НАЦИОНАЛНО ЗАКОНОДАТЕЛСТВО В ОБЛАСТТА НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ***

-Конституция на Република България

-Закон за защита на личните данни (обн. ДВ. бр.1 от 4 януари 2002г., изм. ДВ. бр.57 от 13 юли 2007г.)

-Правилник за дейността на комисията за защита на личните данни и нейната администрация (обн. ДВ. бр.11 от 10 февруари 2009 г.)

-Закон за министерството на вътрешните работи (обн. ДВ. бр.17 от 24 февруари 2006г., изм. ДВ. бр.98 от 14 ноември 2008г., изм. ДВ. бр. 93 от 24 ноември 2009г.)

-Наредба № Із-1187 от 26 юни 2007 г. за реда за извършване на полицейска регистрация

-Инструкция № Із-381 от 10 март 2009 година за реда за обработка на лични данни в Министерството на вътрешните работи (обн. ДВ. бр. 23 от 27 март 2009г.; изм. ДВ. бр. 39 от 26 май 2009г.) – предстои актуализация

**КЗЛД** се състои от председател и четирима членове, които се избират от Народното събрание по предложение на Министерския съвет за срок от 5 (пет) години. Комисията е постоянен орган и е подпомагана от администрация. По-нататъшен напредък в законодателството е постигнат с влизането в сила през м. декември 2002 на **Правилника за прилагане на закона за защита на класифицираната информация**. През 2003 г. е приет **Правилник за дейността на Комисията за защита на личните данни** и на нейната администрация. Започнато е обучение по региони и разговори с професионални организации. Събрани са данни и е протекла процедурата по подаване на заявления за регистрация на администраторите на лични данни в Комисията.

**Комисията се създава на основа на разпоредбите на Закона за защита на личните данни. Тя е независим държавен орган, който защитава интересите на гражданите при обработването на личните им данни и осъществяването на достъпа до тях. Законът изисква председателят на комисията да бъде правоспособен юрист, а членовете и да имат висше юридическо образование или да са магистри по информационни технологии. Членовете на органа трябва да имат 10 годишен стаж по специалността си.**

***В дейността на комисията влизат:***

**- анализ и осъществяване на цялостен контрол   по спазването на нормативните актове в областта на защитата на личните данни;**

**- водене на регистър на администраторите на лични данни;**

**- извършване на проверки на администраторите на лични данни;**

**- изразява становища и дава разрешение в предвидините от закона случаи;**

**- издава задължителни предписания до администраторите във връзка със защитата на личните данни;**

**- може да налага временна забрана за обработване на лични данни, с които се нарушават нормите за защита на личните данни;**

**- разглежда жалби срещу администраторите във връзка с отказан достъп на физическите лица до техните лични данни, както и жалби на други администратори или на трети лица във връзка с правата им предвидени във закона;**

**- участва в подготовката на нормативни актове, свързани със защита на личните данни;**

**- издава бюлетин, в който публикува информация за своята дейност;**

**Според данните представени за 2007 година в бюлетина на Комисията става ясно, че най-голяма част от прверките на администратори (около 40%) са в здравеопазването, на второ място са проверките в образованието, следват потребителските услуги и едва на пето място е държавната администрация. На заседание от 25 юни 2007 е решено да се направят проверки и в банковия сектор, като те са стартирали през септември. С тази преоверка се цели да се покажат слабите места на защита на личнтие данни ако има такива.**

Няколко тенденции се открояват от посочените казуси във връзка с личните данни. Прави впечатление първо тенденцията на завишена защита на личната информация касаеща публичните личности и свързаната с това, както някой я наричат, “култура на секретност”, все още осезаемо присъстваща в Българското общество. Режимът на секретност и потайност на обществени данни, който демократичното управление изисква по принцип да бъде изключение, у нас изглежда не се разбира точно по този начин.

Друга тенденция е използването на законодателството за защита на личните данни, както и за защита на класифицираната информация от институциите за мотивиране на техните откази, т.е. под прикритието на личните данни. Администрацията все по-често започва да използва ЗЗЛД като оправдание за непредоставянето на достъп, под предлог че права на други граждани ще бъдат засегнати по този начин, без, например, да се търси алтернативно правомерно решение. Прави впечатление и желанието за защита на държавните институции от “любопитството” на медиите, като за целта отново се използва прикритието на личните данни.

**Съставените актове за нарушения от друга страна са разделени по сектори, като по ¼ от тях се падат на финансовия сектор и потребителските услуги. В значително по-малка степен са установени нарушения в сектори като телекомуникацията и държавните услуги (по 8%) въпреки огромния шум и насоченото обществено внимание по повод спора за личните данни точно в тези сектори. Визирам все още неясното положение на досиетата наследство от Държавна сигурност и проблема за съхранението на разговорите от мобилните оператори.**

**Най-често срещани нарушения от комисята са непредприемане на необходимите мерки за защита на личните данни от случайно унищожаване, загуба, неправомерен достъп, изменение или разпространение и др. Също така нередности има поради запазването на данните след постигането на целта на обработването им.**

**След разясняването на основнтие понятия в областта на защитата на личните данни, по специално внимание може да обърнем на опасностите в тази сфера при учениците.Поради не толкова честите контакти на учениците със здравеопазването и финансовия сектор, те не са толкова застрашени от неправомерно използване на личнтие им данни в тази сфера. Основните опасности за тази възрастова група идват от защитата на данните им при използването на интернет. С особенно внимание трябва да подхождат към контактите си в мрежата, доста често с непознати хора и даването на лична информация на тези хора.**

**Също така редица сайтове изискват регистрации, от които в последствие информацията въведена там се използва не по предназначение. Пример за това е стотиците нежелани писма с реклами изсипващи се в електронните пощи (така наречения спам). Не е малка съшо така и опасността от вируси, дебнещи навсякъде в интернет, доста от които са създадени да проникнат в компютъра ви и да набавят на създателя им нужната му информация (троянски кон).Като цяло е нужно по-голямо внимание от страна на потребителите, подбиране на контактите и използване на доказано сигурен softwear за предпазване от външни атаки.**

***Нужда от законодателно разрешение на проблема***

Към този момент решението на конфликта между двете права - защитата на личните данни и достъпа до обществена информация, се прави спорадично, по единични случаи, и липсва уеднаквяване на практиките в това отношение. Много често, както се вижда от описаните примери, конфликтът се решава не в полза на общественото знание, а в полза на “културата на секретност”.Истинското разрешение на въпроса кои лични данни, поради това че представляват обществен интерес, следва да бъдат достъпни за гражданите, трябва да стане чрез категорично и недвусмислено решение на законодателно ниво.

Това следва да важи относно основните категории лични данни на обществените служители, като за всички останали конкретни случаи и многообразие от възможни казуси, които не биха могли да се обхванат цялостно от законодателството, би следвало да се остави на съдебните органи да извършат баланса между конкуриращите се права и да прилагат теста за пропорционалност на ограничението върху личната неприкосновеност на служителите.

**Източници на информация:**

* **Конвенция № 108 (1998г.)**
* **Национален план “Партньорство за присъединяване “ (1999г.)**
* **“ Закон за защита на личните данни” (2001г.)**