



**ЕТИЧЕН КОДЕКС НА
„ДЕЛТАСТОК ЗАСТРАХОВАТЕЛЕН БРОКЕР” ООД**

София,
Октомври 2019

СЪДЪРЖАНИЕ

I.	ОСНОВНИ ПОЛОЖЕНИЯ. ЦЕЛИ НА ДОКУМЕНТА	4
II.	ОСНОВНИ ПРИНЦИПИ ПРИ ОБРАБОТКА НА ЛИЧНИ ДАННИ	4
1.	Законосъобразност и яснота	4
2.	Ограничаване до специфична цел	5
3.	Прозрачност	5
4.	De minimis – принцип	5
5.	Унищожаване	5
6.	Фактическа точност и актуалност	5
7.	Конфиденциалност и опазване	6
III.	НАДЕЖДНОСТ НА ИЗВЪРШВАНАТА ОБРАБОТКА НА ДАННИ	6
1.	Лични данни на клиенти и бизнес партньори	6
1.1.	Обработка на данни за целите на договорни отношения	6
1.2.	Обработка на данни за рекламни/маркетингови цели	7
1.3.	Обработка на данни въз основа на законово задължение	7
1.4.	Обработка на данни въз основа на легитимен интерес	7
1.5.	Обработка на (силно) чувствителни данни	8
1.6.	Автоматизирани индивидуални решения	8
1.7.	Потребителски данни и интернет	8
2.	Лични данни на персонал	9
2.1.	Лични данни за целите на трудовите правоотношения	9
2.2.	Обработка на данни въз основа на законово правомощие	9
2.3.	Колективни споразумения за обработка на данни	9
2.4.	Съгласие за обработване на данни	9
2.5.	Обработка на данни въз основа на легитимен интерес	10
2.6.	Телекомуникация и интернет	10
IV.	ТРАНСФЕР НА ЛИЧНИ ДАННИ	10
V.	ДОГОВОР ЗА ОБРАБОТКА НА ДАННИ	11
VI.	ПРАВА НА СУБЕКТИТЕ НА ДАННИ	12

1.	Уведомяване и право на достъп	12
2.	Коригиране.....	12
3.	Възражение.....	12
4.	Ограничаване	12
5.	Изтриване и „забравяне“.....	12
6.	Преносимост.....	13
VII.	КОНТРОЛ ВЪРХУ ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ	13
VIII.	ОТГОВОРНОСТ И САНКЦИИ	13
IX.	ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ	13

I. ОСНОВНИ ПОЛОЖЕНИЯ. ЦЕЛИ НА ДОКУМЕНТА

Като част от социално отговорните принципи, които БРОКЕРЪТ следва по отношение на своите клиенти, служители, външни сътрудници, бизнес партньори и други субекти от външната среда, Дружеството е силно ангажирано с пълното съответствие на своите политики по управление с приложимото национално¹ и европейско² законодателство в сферата на защита на личните данни.

Доверието в Дружеството и цялостната му дейност от страна на всички субекти – пряко свързани с него, както и външни такива, е основна ценност, върху която се гради неговото управление. Опазването репутацията на Дружеството, като едно от най-важните му предимства, също се нарежда сред неговите основни цели.

С оглед на горното Дружеството, разработи и прилага този Етичен кодекс, базиращ се на глобално възприети и общоприети основни принципи и стандарти при работа с лични данни, които целят тяхната надеждна защита.

За работещите в и за Дружеството настоящият Етичен кодекс се привежда в действие със силата на, и е еквивалентен на, всички останали закони в страната, като от служителите без изключение се изисква да съблюдават и да се придържат към етичните правила и стандарти, заложиени в него. Тяхното нарушаване се третира като тежко нарушение, уронващо престижа и доброто име на Дружеството и се взема изключително строго под внимание.

Настоящият Етичен кодекс подлежи на актуализация и може да бъде променян и допълван периодично, когато законодателният напредък налага това. Неговата най-актуална версия може да бъде открита публикувана на уеб-страницата на БРОКЕРА³:

II. ОСНОВНИ ПРИНЦИПИ ПРИ ОБРАБОТКА НА ЛИЧНИ ДАННИ

1. Законосъобразност и яснота

Когато лични данни биват обработвани, индивидуалните права и свободи на субектите⁴ следва да бъдат защитавани. Всякакви лични данни трябва да бъдат събирани и обработвани по законосъобразен и ясен за субектите начин.

¹ Закон за защита на личните данни; Наредба № 1/2013г.

² Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 година, относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (GDPR)

³ <https://www.delatstockins.bg>

⁴ Физическите лица, за които се отнасят личните данни

2. Ограничаване до специфична цел

Лични данни могат да бъдат обработвани само и единствено за целта/целите, която/които са били предварително изрично определени, т.е. преди данните да бъдат събрани. Последващи изменения на първоначалните цели са възможни само в ограничена степен и само ако бъдат мотивирани и обосновани.

3. Прозрачност

Субектите следва да бъдат информирани относно стандартите, по които техните данни ще бъдат и са обработвани. Като общо правило, личните данни трябва по възможност да бъдат събирани директно от физическите лица, които идентифицират и до които се отнасят, а не посредством трети лица. Когато се събират данни, субектът им трябва да бъде или наясно със, или уведомен относно:

- Самоличността на администратора;
- Целта на обработването;
- (Категории) Трети лица, на които е възможно да се трансферират техни данни.

4. De minimis – принцип

Преди започване обработка на лични данни следва да се идентифицира дали и до каква степен обработката на съответния набор от лични данни е необходима, за да бъде постигната на практика целта, за изпълнението на която се предприема. Доколкото целите на обработването биха го позволили, и в случай че не би породило несъразмерни разходи, следва да бъдат използвани анонимизирани или статистически данни. Лични данни не могат и не следва да бъдат събирани и/или съхранявани предварително за потенциални бъдещи цели, освен ако това не е законово допустимо.

5. Унищожаване

Лични данни, които са изпълнили целите, за които са били предназначени и/или които след изтичането на законови или свързани с бизнес процесите срокове вече не са необходими, трябва да бъдат унищожени. В отделни случаи, когато има индикация за интереси, които изискват да бъдат защитени или пък исторически/архивен аспект на такива данни, допустимо е данните да бъдат съхранени на хартиен/електронен носител, докато посоченият казус не се изясни и реши.

6. Фактическа точност и актуалност

Личните данни на електронни носители, а когато е възможно и на хартиени, следва да бъдат коригирани и допълвани, в случай че се появи необходимост от тяхната актуализация. Трябва да се предприемат подходящи и навременни стъпки, за да се

гарантира, че неточни или непълни, или неверни лични данни са изтрити, коригирани, допълнени или актуализирани.

7. Конфиденциалност и опазване

Личните данни са абсолютен обект на конфиденциалност и трябва да бъдат пазени поверително, да бъдат третираны като конфиденциална информация на лично ниво и да бъдат защитавани с подходящи и приложими организационни, и технически мерки с цел предотвратяване на неоторизирано достъпване, неправомерно обработване от страна на трети лица, както и внезапна загуба или унищожаване.

Отделно от изброеното по-горе, в цялостната си дейност Дружеството следва социално отговорна политика, която се изразява и в осигуряване на стабилно и възходящо развитие на бизнеса, което всички работещи в и за Дружеството приемат като своя първостепенна отговорност пред обществото. Въпреки това, обаче, в дейността на Дружеството следва да се съблюдава принципът *primum non nocere* (*преди всичко да не се вреди*). В допълнение, при необходимост от тълкуване на нормативно изискване и при всякакви други решения и действия в рамките на закона, същите следва да се базират на върховенството на морала и професионалната етика. Дружеството уважава и подпомага защитата на човешките права в международен план, в това число и на правото на неприкосновеност и личен живот.

Абсолютно забранена практика в Дружеството е задържането на документи за самоличност на каквито и да било категории физически лица, както и на копия от такива документи.

III. НАДЕЖДНОСТ НА ИЗВЪРШВАНАТА ОБРАБОТКА НА ДАННИ

Събирането, обработването и употребата на лични данни са разрешени само въз основа на изброените по-долу правни основания. Наличието на едно от тези правни основания е също така задължително, ако първоначалната цел за събиране, обработване и употреба на личните данни трябва да бъде променена.

1. Лични данни на клиенти и бизнес партньори

1.1. Обработка на данни за целите на договорни отношения

Личните данни за потенциални клиенти, настоящи клиенти и бизнес партньори, както и всякакъв тип контрагенти могат да бъдат обработвани, за да се сключи, изпълни и/или прекрати съответен договор. Това обхваща и извършването на незаплатени консултантски услуги за съ-контрагента, в случай че е свързано с целите и изпълнението на договора. Преди самото сключване на договора – по време на предварителната (преддоговорна фаза) – лични данни могат да бъдат обработвани, за да се подготвят оферти или възлагателни писма, или за да се

изпълнят други изисквания на потенциалните клиенти, които се отнасят пряко до последващото сключване на договор, независимо дали такъв бъде реално сключен или не. Потенциалните клиенти могат да бъдат контактувани по време на процеса по подготовка на договора, като се използва информация за физически лица, която е била предоставена на Дружеството от същите. В тази връзка трябва да се съблюдават всякакви ограничения, предварително зададени/изискани от потенциалните клиенти. За извършването на каквито и да било рекламни действия извън потенциалното възлагане, следва да бъдат спазени задълженията съгласно чл. III.1.2 от този Етичен кодекс.

1.2. Обработка на данни за рекламни/маркетингови цели

Ако бъде поискана информация от страна на потенциален клиент (например: запитване относно информация за услуги в дадена област), работата с разкрити по този начин данни, за да се отговори на такова запитване, е разрешена.

Отделно от това, обаче, субектът на данните трябва да бъде информиран за какво ще бъдат използвани неговите/нейните данни, в частност ако данните ще бъдат съхранявани само за рекламни цели. Субектът на данните трябва да бъде информиран, че предоставянето на данните за рекламни, маркетингови и/или статистически цели е доброволно. Това съгласие трябва да бъде получено при комуникация със субекта, като му се даде възможност за избор на начина, по който Дружеството ще се свързва в бъдеще – обикновена поща, електронна поща, други средства за масова комуникация и/или телефон.

В случай че субектът на данните откаже същите да бъдат използвани по-нататък за рекламни цели, данните не могат да бъдат използвани за тези цели и трябва да бъдат блокирани за употреба за тези цели.

Съгласието може да бъде получено в писмена или електронна форма, под формата на декларация, за целите на документацията и доказателствени цели. При някои обстоятелства съгласие може да бъде получено и устно, така например по време на телефонен разговор, при условие че запис от разговора се съхранява за доказателствени цели.

1.3. Обработка на данни въз основа на законово задължение

Обработката на лични данни е също така разрешена, когато това се изисква съгласно действащото българско законодателство. Методът и обхватът на обработване следва да бъдат необходими условия за изпълнение на законовото задължение, а съответните императивни нормативни разпоредби следва да бъдат съобразени при извършване на обработването.

1.4. Обработка на данни въз основа на легитимен интерес

Лични данни могат също така да бъдат обработвани, ако това се явява необходимо условие за защита на легитимните законови интереси на Дружеството. Такива

интереси най-общо казано и обичайно са или от правен характер (например събиране на вземания) или от търговско естество (например недопускане на договорно неспазване). В отделни случаи, когато интересът на субекта на данните заслужава по-силна защита и се ползва с предимство, Дружеството няма право да обработва лични данни на основание по тази т. 1.4. Преди данните да бъдат обработени, задължително следва да се определи дали има такива индивидуални интереси, които биха се ползвали с по-голяма защита.

1.5. Обработка на (силно) чувствителни данни

По общо правило, (силно) чувствителни⁵ данни могат да бъдат обработвани, само ако законът изисква това или субектът на личните данни е дал своето изрично съгласие. Такива данни могат да бъдат обработвани и ако това е необходимо за подаване и защита на искове срещу, или пък в полза на и предвид конкретно възлагане от страна на субекта на данните. При планирана обработка на (силно) чувствителни данни желателно е да се информира предварително Длъжностното лице по защита на лични данни.

1.6. Автоматизирани индивидуални решения

Автоматизираната обработка на лични данни, която би могла да бъде използване за определяне/конкретизиране на дадени аспекти (например оценка на клиентите при заявяване на застрахователна услуга) в никакъв случай не може и не следва да бъде единственият критерий при вземане на решения, които биха имали негативни правни последици или биха могли сериозно да навредят на субекта на данни.

1.7. Потребителски данни и интернет

Ако лични данни се събират и използват от уебсайтове или от приложения, субектите следва да бъдат информирани за това посредством декларация за поверителност, а когато е приложимо и посредством информация за протокол за пренос на хипертекст „бисквитки“ (*HTTP cookies*). Декларацията за поверителност и всякаква информация за „бисквитки“ следва да бъде поместена по такъв начин, че да бъде лесно разпознаваема, директно достъпна и винаги на разположение на субектите. Ако са създадени потребителски профили (проследяващи „тракери“) с цел изчисляване на потреблението на уебсайтовете и/или приложенията, субектите на тези лични данни задължително трябва да бъдат информирани за това чрез декларацията за поверителност. Такъв тип проследяване може да се извършва, само ако е допустимо съгласно българското законодателство или след даването на изрично съгласие от страна на физическото лице.

⁵ Съгласно нормата на чл. 5, ал. 1 от ЗЗЛД (*здравен статус, сексуална ориентация, политически възгледи, расово-етнически произход и др.*)

2. Лични данни на персонал⁶

2.1. Лични данни за целите на трудовите правоотношения

Във връзка с трудовите правоотношения лични данни могат да бъдат събирани и обработвани, винаги когато това е необходимо за инициране/започване, продължаване и/или прекратяване на такова трудово правоотношение, като това се отнася и за граждански договори за (постоянна) работа.

Когато се „поставя начало“ на трудово правоотношение, личните данни на кандидата за работа могат да бъдат обработвани, а в случай че същият бъде отхвърлен, неговите/нейните данни трябва да бъдат изтрети при спазване на евентуален задължителен или желан период на съхранение, освен ако кандидатът не се е съгласил информацията за него/нея да бъде съхранявана от Дружеството за бъдещ процес по подбор на персонал.

По отношение на вече съществуващо трудово правоотношение обработването на личните данни на служители трябва винаги да се отнася до целите на трудовия/гражданския договор. Когато обработката се извършва по начин, който излиза извън целите на изпълнението на трудовия договор, трябва да е налице друго правно основание за тази обработка. Това може да включва законови задължения на Дружеството, колективни решения, взети с представители на служителите, съгласие на служителя или легитимен интерес на Дружеството.

2.2. Обработка на данни въз основа на законово правомощие

Обработката на лични данни на служители е позволена, ако такава е задължителна, изискуема или позволена съгласно действащото българско законодателство при стриктно съблюдаване и спазване на съответните законови разпоредби.

2.3. Колективни споразумения за обработка на данни

Ако действията, свързани с обработка на лични данни на служители, надвишава обхвата на целите по изпълнението на трудовия/гражданския договор, обработката въпреки това е допустима, ако е позволена въз основа колективно споразумение.

2.4. Съгласие за обработване на данни

Отделно от горната точка 2.3., лични данни на служителите могат да бъдат обработвани и при дадено съгласие на физическото лице. Декларацията за съгласие трябва да бъде подадена доброволно, като не се счита, че наличието на трудово правоотношение и йерархичната субординация на служителите сама по себе си нарушава доброволния характер на дадено съгласие. Декларацията за съгласие следва да бъде получена в писмена или електронна форма за целите на документалност.

⁶ Служители както на трудови, така и на граждански договори.

2.5. Обработка на данни въз основа на легитимен интерес

Лични данни на служители могат да бъдат обработвани извън обхвата на трудовите взаимоотношения и при наличието на легитимен правен интерес на Дружеството. Мерки за контрол на работното място, които изискват обработване на лични данни на служители, могат да бъдат предприети, само ако Дружеството е законово задължено или има основателна причина, като тези мерки трябва да бъдат уместни и пропорционални на законовите интереси на служителите.

2.6. Телекомуникация и интернет

Телефонното оборудване, електронните адреси, интранет и интернет, както и всички достъпни социални мрежи се предоставят от Дружеството преди всичко за изпълнение на задачи, свързани с работата и трудовите задължения и представляват ресурс на Дружеството. Те трябва да бъдат използвани по начин, че да не нарушават приложимите нормативни регулации и вътрешни корпоративни правила. В случай че е позволено тяхното ползване за лична употреба, следва да бъдат съобразени всякакви разпоредби, отнасящи се до конфиденциалност и пазене на професионална тайна.

Общ надзор над онлайн и телефонен трафик, и употреба няма да бъде извършван от страна на Дружеството, но с цел навременна защита от кибер атаки индивидуални профили могат да бъдат следени, ако това е необходимо, както и да бъдат блокирани отделни домейни с технически вредоносно съдържание.

IV. ТРАНСФЕР НА ЛИЧНИ ДАННИ

Извършването на трансфер на лични данни на получатели извън Дружеството става при спазване на изискванията за получаване на разрешение за обработка на лични данни, поместени в Раздел III от този Етичен кодекс. Получателите на личните данни трябва да бъдат задължени да използват данните само за конкретно и предварително определените цели.

Ако личните данни се трансферират към Европейския съюз/Европейското икономическо пространство или трета държава, Дружеството трябва да сътрудничи при всякакви проверки, извършвани от надзорния орган – КЗЛД, и следва да се съобрази с всякакви насоки, дадени от надзорния орган с оглед получаване на разрешение за осъществяване на трансфера.

Ако получателите са част от международна сертифицирана система за обвързващи корпоративни правила за защита на данни, от получателите се очаква да гарантират, че ще съдействат на съответните местни надзорни органи.

Участието в такава сертифицирана система трябва задължително да бъде съгласувано с Длъжностното лице по защита на личните данни на Дружеството.

V. ДОГОВОР ЗА ОБРАБОТКА НА ДАННИ

Обработката на данни „от Името на“ означава, че Дружеството обработва определени лични данни във връзка с дадено възлагане, без да му се приписва отговорността за свързаните с тази обработка бизнес процеси. В този случай възложителят в качеството му на администратор на личните данни продължава да носи пълната отговорност за тези данни. Дружеството, от своя страна, има право да обработва данните единствено съобразно инструкциите на възложителя.

Когато пък Дружеството сключва договор с лице – обработващ лични данни, по силата на който ще предоставя на това лице лични данни, а то ще ги обработва от Името на Дружеството, трябва да бъдат съобразени и изпълнени следните изисквания:

- 1.** Обработващият се избира въз основа на способността му за покриване и изпълнение на необходимите нормативно-изискуеми технически и организационни мерки за защита на личните данни.
- 2.** При обработване на лични данни от страна на външно лице от името на Дружеството това трябва да бъде регламентирано в писмен вид и възложен по силата на съответен договор, в който да бъдат документиран целите за обработка на данни и отговорностите на обработващия.
- 3.** Преди да се инициира обработката на данните, Дружеството трябва да се увери, че обработващият наистина ще се съобрази със задълженията си за защита на личните данни. Обработващият може да докаже съответствието си с изискванията за защита на данните по-специално чрез представяне на съответна призната сертификация.
- 4.** В случай на трансгранично обработване на данни трябва да бъдат изпълнени националните изисквания за разкриване на лични данни в чужбина. В частност, личните данни, трансферирани от Дружеството, могат да бъдат обработвани от трети държави, само ако обработващият може да докаже, че неговите стандарти за защита на данни са еквивалентни на стандартите по този Етичен кодекс.

Подходящи доказателствени инструменти са следните:

- a)** Споразумение относно стандартни договорни клаузи на ЕС за обработка на данни;
- b)** Участие на обработващия в сертифицирана система, акредитирана от ЕС за осигуряване на достатъчно ниво за защита;
- c)** Признаване на обвързващи корпоративни правила на обработващия за създаване на подходящо ниво от надзорния орган за защита на данни; или

- d) Решение за адекватно ниво на защита на Европейската комисия за конкретна държава.

VI. ПРАВА НА СУБЕКТИТЕ НА ДАННИ

1. Уведомяване и право на достъп

Физически лица могат да изискат информация от Дружеството за личните данни, отнасящи се до тези физически лица, които се съхраняват реално от Дружеството; за начина, по който са били събрани първоначално; за какви цели се обработват и др. В случай че лични данни за лицето, отправило запитването, се трансферират на трети лица, трябва да бъде разкрита и информацията относно идентичността на получателя или категориите получатели на личните данни.

2. Коригиране

Ако се установи от субект на лични данни, че данните, събирани и съхранявани за него, са неверни или непълни, субектът може да поиска тяхното незабавно коригиране и актуализиране.

3. Възражение

Физическото лице има право по всяко време да възрази срещу обработка на негови лични данни, която се базира на профилиране и/или автоматично взети решения.

Ако Дружеството не е в състояние да обясни логиката, която седи зад това автоматично взето решение или пък да обоснове убедителни законови основания, които да имат предимство пред правата и интересите на субекта на данните, Дружеството следва да преустанови без излишно забавяне такъв тип обработване на личните данни на конкретния субект, който е възразил срещу него.

4. Ограничаване

Субект на лични данни може да поиска от Дружеството ограничаване на категориите лични данни, които Дружеството съхранява и обработва за него/нея, или видовете обработване, които Дружеството извършва, с оглед конкретни индивидуални обстоятелства, а то следва да ги вземе предвид и да се съобрази с тях, освен ако има нормативни задължения за този вид обработка на тези категории лични данни. Същото право на ограничаване се отнася и до случаи на неправомерно обработване, когато същото не е необходимо, но субектът не желае пълно изтриване на личните си данни, а само ограничаване на тяхното използване от страна на Дружеството.

В случай че данните на дадено физическо лице се обработват за рекламни, търговски и/или маркетингови цели, то има неограниченото право да поиска незабавното блокиране на личните си данни за тези цели.

5. Изтриване и „забравяне“

В случай че лични данни се обработват от страна на Дружеството без правно основание или са били правомерно събрани, но правното основание впоследствие е отпаднало, или целите, за които са били събрани и обработвани данните, са вече изпълнени и не са с продължително действие, или субектът оттегля своето изрично съгласие за по-нататъшна обработка, физическото лице може да поиска изтриване на свързаните с него лични данни без ненужно забавяне.

6. Преносимост

Физическите лица имат право да поискат от Дружеството да предостави и директно да прехвърли събрани и съхранявани за тях лични данни на друг администратор на лични данни, в случай че събираните за това лице данни се обработват автоматизирано и (кумулятивно условие) въз основа на съгласие, дадено от страна на физическото лице или изпълнение на договорно задължение.

VII. КОНТРОЛ ВЪРХУ ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

Длъжностното лице по защита на личните данни упражнява контрол, като следи регулярно за спазване на този Етичен кодекс, на актуалната Инstrukция на Дружеството за мерките и средствата за защита на личните данни, както и на действащото българско законодателство, регулиращо защитата на личните данни. Резултатите от тези редовни проверки, които се извършват поне веднъж годишно, трябва да бъдат навременно комуникирани с управителя на клона.

VIII. ОТГОВОРНОСТ И САНКЦИИ

Управителните органи на Дружеството са длъжни да осигурят предприемането на организационните и технически мерки, които да отговарят на изискванията за осигуряване на достатъчна защита на личните данни. Съответствие с всички вътрешни правила и взети мерки за осигуряване на адекватна защита е отговорност на всеки отделен служител.

В случай че се извършва проверка на място в офиса на Дружеството от страна на надзорния орган, отговорност на всеки един служител на Дружеството е да се погрижи за незабавното уведомяване на Длъжностното лице по защита на личните данни.

Длъжностното лице по защита на личните данни на Дружеството носи отговорност за надлежната подготовката на служителите и тяхното редовно обучение в областта на защита на личните данни.

IX. ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Този Етичен кодекс е приет с решение на управителя на БРОКЕРА по Протокол № [1] от [01.10.2019] г.