

## **Информация по чл. по чл. 12, ал.4 от Закона за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения (ЗЗЛПСПОИН)**

Във връзка с влизането на ЗЗЛПСПОИН в сила, считано от 04 май 2023 г. ЗБ „БИГ БРОКЕР” ЕООД, в качеството си на работодател от частния сектор, който се явява задължен субект по чл. 12, ал. 1 от ЗЗЛПСПОИН предоставя следната информация по чл. 12, ал.4:

### **1. Защита по ЗЗЛПСПОИН се предоставя при следните кумулативни условия:**

Качество на сигнализиращото лице: физическо лице, което подава сигнал или публично оповестява информация за нарушение, станало му известно в качеството му на:

работник, служител, държавен служител или друго лице, което полага наемен труд, независимо от характера на работата, от начина на заплащането и от източника на финансирането;

лице, което полага труд без трудово правоотношение и/или упражнява свободна професия и/или занаятчийска дейност;

доброволец или стажант;

съдружник, акционер, едноличен собственик на капитала, член на управителен или контролен орган на търговско дружество, член на одитния комитет на предприятие;

лице, което работи за физическо или юридическо лице, негови подизпълнители или доставчици; кандидат за работа, участвал в конкурс или друга форма на подбор за постъпване на работа и получил в това качество информация за нарушение;

работник или служител, когато информацията е получена в рамките на трудово или служебно правоотношение, което е прекратено към момента на подаване на сигнала или на публичното оповестяване;

всяко друго сигнализиращо лице, което подава сигнал за нарушение, станало му известно в работен контекст.

На основание чл. 9 ЗЗЛПСПОИН не се образуват производства по анонимни сигнали.

Предметна област на сигналите за нарушения:

Сигналите трябва да се отнасят до нарушения на българското законодателство или на актове на Европейския съюз, посочени в Приложение към чл. 3, ал. 1 и 3 от ЗЗЛПСПОИН – Част I и Част II:

в областта на:

а) обществените поръчки;

б) финансовите услуги, продукти и пазари и предотвратяването на изпирането на пари и финансирането на тероризма;

в) безопасността и съответствието на продуктите;

г) безопасността на транспорта;

д) опазването на околната среда;

е) радиационната защита и ядрената безопасност;

ж) безопасността на храните и фуражите, здравето на животните и хуманното отношение към тях;

з) общественото здраве;

и) защитата на потребителите;

к) защитата на неприкосновеността на личния живот и личните данни;

л) сигурността на мрежите и информационните системи;

нарушения, които засягат финансовите интереси на Европейския съюз по смисъла на чл. 325 от Договора за функционирането на Европейския съюз;

нарушения на правилата на вътрешния пазар по смисъла на чл. 26, параграф 2 от Договора за функционирането на Европейския съюз, включително правилата на Европейския съюз и българското законодателство относно конкуренцията и държавните помощи;

нарушения, свързани с трансгранични данъчни схеми, чиято цел е да се получи данъчно предимство, което противоречи на предмета или на целта на приложимото право в областта на корпоративното данъчно облагане;

извършено престъпление от общ характер, за което лице по т.1.1. е узнало във връзка с извършване на своята работа или при изпълнение на служебните си задължения.

нарушения на българското законодателство в областта на:

а) правилата за заплащане на дължими публични държавни и общински вземания;

б) трудовото законодателство;

в) законодателството, свързано с изпълнението на държавна служба.

### И да не се отнасят до нарушения:

на правилата за възлагане на обществени поръчки в областта на отбраната и националната сигурност, когато те попадат в обхвата на чл. 346 от Договора за функционирането на Европейския съюз;

на защитата на класифицирана информация по смисъла на чл. 1, ал. 3 от Закона за защита на класифицираната информация;

които са станали известни на лица, упражняващи правна професия и за които съществува задължение по закон за опазване на професионална тайна;

на поверителността на здравната информация по смисъла на чл. 27 от Закона за здравето;

на тайната на съдебното съвещание;

на правилата на наказателното производство.

Сигнализиращото лице да е подало сигнал за нарушение чрез вътрешен или външен канал при условията и по реда на ЗЗЛПСПОИН и е имало основателна причина да счита, че подадената от него информация е била вярна към момента на подаването на сигнала.

Защита по ЗЗЛПСПОИН се предоставя и на:

- а) лица, които помагат на сигнализиращото лице в процеса на подаване на сигнал;
- б) лица, които са свързани със сигнализиращото лице и които могат да бъдат подложени на репресивни ответни действия поради сигнализирането;
- в) юридически лица, в които сигнализиращото лице притежава дялово участие, за които работи или с които е свързано по друг начин в работен контекст;
- г) лица, които публично оповестяват информация за нарушения и за която са постъпили данни в КЗЛД или е поискана защита от съответното лице, оповестило информацията.

На основание чл. 9, т. 2 ЗЗЛПСПОИН не се образува производство по сигнали, отнасящи се до нарушения, извършени преди повече от две години.

## 2. Как се подава сигнал?

Начините за подаване на сигнали са чрез:

- - вътрешен канал, който се осигурява от Дружеството;
- - външен канал, който се осигурява от КЗЛД;
- - публично оповестяване на информацията.

За подаване на сигнали чрез вътрешния канал на Дружеството, подаващите сигнали могат да ползват един от следните начини:

- по електронната поща на следния електронен адрес: [signal@bigbroker.bg](mailto:signal@bigbroker.bg)
- по телефон на следния номер: 0887736693 ;
- по пощата или лично на адреса на Дружеството: гр. Плевен, ул. „Васил Левски” № 108, ет.2 За гарантиране поверителността на подадения сигнал при подаване на сигнала на хартиен носител, се препоръчва на подаващия, да постави бележка за поверителност и указание „Пликът да се отвори от лицето, отговорно за разглеждане на сигнали по ЗЗЛПСПОИН“.

При желание от страна на сигнализиращото лице - чрез използване на *образеца на Формуляр за регистриране на сигнал за подаване на информация за нарушения съгласно ЗЗЛПСПОИН*. Формулярът не е задължителен за попълване от сигнализиращото лице. В случай че то реши да го използва обаче, лицето следва да попълни само Част I – V включително и да го подпише: при изпращане на формуляра по пощата – със саморъчен подпис; при изпращане по електронна поща – с квалифициран електронен подпис. Образецът на Формуляр може да бъде намерен [тук](#).

Чрез лична среща със служителя, отговарящ за разглеждането на сигнали, който на място ще документира подадения сигнал чрез попълване на Формуляр за регистриране на сигнал за подаване на информация за нарушения съгласно ЗЗЛПСПОИН.

Когато сигнализиращото лице не използва образеца на формуляр за регистриране на сигнал за подаване на информация за нарушения съгласно ЗЗЛПСПОИН, то може да подаде сигнала писмено по всякакъв друг избран от него начин.

В тези случаи служителят, отговарящ за разглеждането на сигнала, ще установи контакт със сигнализиращото лице с цел попълване на Формуляр за регистриране на сигнал за подаване на информация за нарушения съгласно ЗЗЛПСПОИН.

Всички писмени доказателства, с които сигнализиращото лице разполага, следва да се приложат към сигнала.

### 3. Какъв е редът за разглеждане на подадените сигнали?

Сигналът ще бъде регистриран с уникален идентификационен номер и в 7-дневен срок от получаването му отговорният служител ще потвърди получаването му;

Ако сигналът не отговаря на някое от законовите изисквания за редовност, отговорният служител ще уведоми сигнализиращото лице в какво се състои нередовността и по какъв начин същата би могла да бъде отстранена;

Ще бъде извършена вътрешна проверка по сигнала, като в срок до три месеца от потвърждаването на получаването на сигнала, отговорният служител ще предостави на сигнализиращото лице обратна информация, съдържаща предприетите действия и резултатите от проверката.

### 4. Каква защита се предоставя на сигнализиращите лица?

Забранява се всяка форма на ответни действия спрямо сигнализиращите лица, имащи характера на репресия и поставящи ги в неблагоприятно положение, както и заплахи или опити за такива действия, включително под формата на:

временно отстраняване, уволнение или прилагане на друго основание за прекратяване на правоотношението, по което лице полага наемен труд;

понижаване в длъжност или забавяне на повишение в длъжност;

изменение на мястото или характера на работата, продължителността на работното време или намаляване на възнаграждението;

отказ за осигуряване на обучение за поддържане и повишаване на професионалната квалификация на работника или служителя;

отрицателна оценка на работата, включително в препоръка за работа;

прилагане на имуществена и/или дисциплинарна отговорност, включително налагане на дисциплинарни наказания;

принуда, отхвърляне, заплашване за предприемане на ответни действия или действия, изразени физически, словесно или по друг начин, които имат за цел накърняване на достойнството на лицето и създаване на враждебна професионална среда;

пряка или непряка дискриминация, неравностойно или неблагоприятно третиране;

отнемане на възможност за преминаване от срочен трудов договор на трудов договор за неопределено време, когато работникът или служителят е имал законно право да му бъде предложена постоянна работа;

предсрочно прекратяване на срочен трудов договор или отказ за повторно сключване, когато такава е допустимо по закон;

вреди, включително за репутацията на лицето, по-специално в социалните мрежи, или финансови загуби, включително загуба на бизнес и загуба на доход;

включване в списък, изготвен въз основа на официално или неофициално споразумение, в сектор или в отрасъл, което може да доведе до това лицето да не може да постъпи на работа или да не може да достави стока или услуга в този сектор или отрасъл (черен списък);

предсрочно прекратяване или разваляне на договор за доставка на стоки или услуги, когато лицето е доставчик;

прекратяване на лиценз или разрешение;

насочване на лицето към извършване на медицински преглед;

Комисията за защита на личните данни предоставя безплатни и достъпни информация и съвети на защитените лица.

### 5. Какви са предпоставките за предоставяне на защита по смисъла на ЗЗЛПСПОИН?

За да бъде предоставена защита на сигнализиращото лице, същото следва да е подало сигнала съгласно изискванията на ЗЗЛПСПОИН и да е имало основателна причина да счита, че обективизираната в сигнала информация за нарушението е била вярна към момента на подаването и че тази информация попада в приложното поле по чл. 3 на ЗЗЛПСПОИН.

Съгласно чл. 39 на ЗЗЛПСПОИН засегнатото от сигнала лице има право на обезщетение за всички имуществени и неимуществени вреди, когато е установено, че сигнализиращото лице съзнателно

е подало сигнал с невярна информация или публично е оповестило невярна информация, както и когато според обстоятелствата е било длъжно да предположи, че информацията е невярна.

#### **6. Режим на поверителност:**

Достъп до личните данни, съдържащи се в сигналите за нарушения, имат единствено съответния служител/служители на Дружеството, отговарящи за разглеждането на съответния сигнал при спазване на принципа „необходимост да се знае“ в изпълнение на функционалните задължения и/или конкретно възложена задача.

Сигналите се обработват при спазване на задължението за поверителност, произтичащо от чл. 31 и чл. 32 от ЗЗЛПСПОИН. Не се събират лични данни, които явно не са от значение за разглеждане на конкретния сигнал, а ако бъдат случайно събрани, се заличават (чл. 32, ал. 2 от ЗЗЛПСПОИН).

#### **7. Последващи действия:**

Действията, които Дружеството предприема във връзка с разглеждането на конкретен сигнал, са подробно уредени в Правила на Дружеството за вътрешно подаване на сигнали и за последващи действия по тях.

Съобразно естеството на сигнала и за изясняване на конкретни обстоятелства, служителят/служителите, отговарящи за разглеждането на сигнала, имат задължение да поддържат връзка със сигнализиращото лице и да му предоставят обратна информация за предприетите действия.

#### **8. Условия за защита срещу носене на отговорност в случай на нарушаване на поверителността по чл. 31 от ЗЗЛПСПОИН:**

Сигнализиращите лица се освобождават от отговорност при условията на чл. 36 от ЗЗЛПСПОИН, както следва:

лицето е сред кръга от лица по чл. 5, ал. 2 и ал. 3 от ЗЗЛПСПОИН;

сигналът се отнася за нарушение по чл. 3 от ЗЗЛПСПОИН;

когато придобиването на информацията за твърдяното нарушение или достъпа до нея не съставлява самостоятелно престъпление;

са имали основателна причина да считат, че подаването на сигнала или публичното оповестяване на информация е било необходимо за разкриване на нарушението, независимо от наличието на ограничения за разкриването на съответната информация, вкл. когато тази информация съдържа търговска тайна.

***Настоящият информационен материал има за цел да даде разяснения по принципни въпроси по приложението на Закона за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения. Същият не претендира за изчерпателност.***

## **Уведомление за поверителност относно функционирането на вътрешен канал на Дружеството за подаване на сигнали по реда на закона за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения**

Дружеството се ангажира със защитата на личната неприкосновеност на лицата, които са част от екипа на дружеството (ръководители, служители, стажанти) или са негови партньори (доставчици на услуги).

### **1. Какви са целите на обработване на лични данни?**

Лични данни се обработват с цел образуване на вътрешно производство за разглеждане и предприемане на мерки по подадени сигнали за твърдени нарушения, извършени от служители на Дружеството.

Нарушенията, предмет на подадени сигнали, могат да бъдат нарушение на българското законодателство и/или на законодателството на Европейския съюз в областта на: финансовите услуги, продукти и пазари и предотвратяването на изпирането на пари и финансирането на тероризма; защитата на потребителите; защитата на неприкосновеността на личния живот и личните данни; сигурността на мрежите и информационните системи; трудовото законодателство; други, посочени в чл. 3 ЗЗЛПСПОИНВ.

### **2. На какво основание се обработват лични данни на сигнализиращите лица и лицата, за които се твърди, че са извършили нарушение?**

Личните данни на сигнализиращите лица и лицата, за които се твърди, че са извършили нарушение се обработват в изпълнение на нормативните задължения на Дружеството, предвидени в ЗЗЛПСПОИН.

### **3. Какви лични данни се обработват и по какъв начин се събират същите?**

Дружеството обработва само такива лични данни, които са строго необходими за целите на разглеждане и предприемане на мерки по подадени сигнали за твърдени нарушения от служителите на дружеството.

Данните се получават от подадените сигнали по вътрешния канал на дружеството, като в процеса на проверка и предприемане на мерки по сигнала същото може да обработва следните лични данни:

имена, заемана длъжност, телефонен номер, електронна поща и други данни за контакт на сигнализиращото лице;

имена, заемана длъжност, телефонен номер, електронна поща и други данни за контакт на лице сочено като нарушител в подаден сигнал;

имена, заемана длъжност и данни за контакт на лицата, проверяващи сигнала;

лични данни, предоставени във връзка с обстоятелствата, които са предмет на сигнала и такива събрани при неговата проверка;

лични данни, събрани при извършването на проверка по сигнала.

### **4. На какво основание се обработват лични данни на сигнализиращите лица?**

Личните данни, събрани във връзка с получен сигнал за нарушение (и особено данни за самоличността на лицето, подало сигнала) се обработват при условията на пълна конфиденциалност, съгласно императивните изисквания на ЗЗЛПСПОИН.

Тези лични данни ще бъдат на разположение на определените от Дружеството служители, отговарящи за разглеждането на сигналите по смисъла на чл. 14 ЗЗЛПСПОИН. Тези лица са специално обучени и наясно със задължението си за конфиденциалност относно всички аспекти на проверката.

Дружеството би могло да разкрие лични данни на сигнализиращо лице, когато това се изисква от закона или когато е налице обосновано убеждение, че такова разкриване е необходимо за защита

на законните права на дружеството и/или за спазване на искане от надзорна институция или друг административен или съдебен орган.

#### **5. Трансферира ли се лични данни извън Република България?**

Дружеството няма да предава лични данни на сигнализиращи лица извън територията на Република България.

#### **6. Какъв е периодът на съхранение на личните данни?**

Дружеството съхранява лични данни толкова дълго, колкото е необходимо за целите на проверка на сигнала или ако е приложимо, за налагане на санкции или съобразяване с нормативно изискване. Дружеството има законен интерес да съхранява лични данни до изтичане на съответните давностни срокове за предявяване на претенции (5 години).

След изтичането на посочените срокове, Дружеството ще изтрие или анонимизира съхраняваните лични данни, освен ако те са необходими за висящо съдебно, административно производство или производство по разглеждане на депозирана пред дружеството жалба.

Анонимизирането е алтернатива на изтриването на данните и представлява процес, при който всички лични разпознаваеми данни (данни, които позволяват идентифицирането на лицето), се заличават необратимо. Анонимизираните данни не представляват лични и спрямо тях не се прилагат нормативни изисквания за изтриване.

#### **7. Как Дружеството защитава личните данни?**

Дружеството прилага различни организационни и технически мерки, за да гарантира, че обработваните лични данни са защитени и запазени поверителни. Дружеството разполага със системи и процедури за предотвратяване на неототоризиран достъп, неправилно модифициране или оповестяване, злоупотреба или загуба на информация. Личните данни се защитават посредством физически, електронни и процедурни мерки и правила в съответствие с приложимите закони и разпоредби. Част от мерките, които се прилагат за осигуряване на високо ниво на сигурност по отношение на управлението на личните данни, включват, наред с други и следните:

Минимизиране - личните данни, които се изискват, са уместни и са ограничени само до това, което е необходимо във връзка с целите, за които се обработват;

Строг вътрешен контрол върху достъпа до лични данни - достъпът личните данни е разрешен само на тези наши служители, които се нуждаят от тази информация, за да упражняват правилно своите професионални задължения;

Проверка на проникването (Penetration testing) – прилага се ототоризирана симулационна атака на определена компютърна система, извършена за оценка на сигурността на тази система. Редовното тестване за сканиране и проникване се използва, за да се идентифицират евентуални уязвимости в сигурността и да се приложат съответните средства за отстраняването им; Осигуряване на текущо обучение по защита на личните данни на всички служители на дружеството и постоянен вътрешен контрол по прилагането на мерките за поверителност. Само лица, изрично определени за проверка на получен сигнал и на последващ етап представляващите дружеството ще имат достъп до лични данни на сигнализиращото лице, съдържащи се в сигнала.

#### **8. С какви права разполагат лицата?**

Право на достъп до личните данни, свързани с лицето;

Право на възражение срещу обработването на личните данни, когато дружеството се позовава на свой легитимен интерес;

Право на корекция на неточните личните данни, свързани с лицето;

Право на изтриване на личните данни, свързани с лицето („правото да бъдеш забравен“);

Право на ограничаване на обработването на личните данни, свързани с лицето;

Право на достъп до личните данни и да се използват отново посредством прехвърляне на друг администратор („право на преносимост“);

Право на жалба до Комисията за защита на личните данни, с адрес гр. София, п. код 1592, бул. „Цветан Лазаров“ № 2. Може да се потърси защита и по съдебен ред.