

15.12.2023г., Сливен

До всички служители на РЕТАЛ БАЛКАН ЕООД

Уважаеми колеги!

С удоволствие ви съобщаваме приемането на Политиката за вътрешно докладване („Политика/та“), съществена стъпка към осигуряването на прозрачност, съответствие и защита на лицата подаващи сигнали за нарушения в рамките на дружеството РЕТАЛ БАЛКАН ЕООД („Дружество/то“).

Политиката е разработена вследствие приемането на Директива (ЕС) 2019/1937 на Европейския парламент и Съвета, от 23.10.2019г., относно защитата на лица, които подават сигнали за нарушения на правото на Съюза, постановяваща унифицирана и солидна рамка за защитата на лица, подаващи сигнали за нарушения на законите на Съюза в страните-членки на Европейския съюз.

Главната цел на това законодателство е да се насърчи докладването на криминални и административни престъпления и други нарушения на законите на Европейския съюз, като се осигуряват правни защитни мерки срещу репресивни действия.

Настоящият документ очертава ключовите разпоредби на Политиката и действието ѝ.

1. Цел: Политиката е разработена в съответствие със Закона за защита на лица, подаващи сигнали или публично оповестяващи информация за нарушения, №11 от 02.02.2023г., с поправките („Законът“), с който Директива (ЕС) 2019/1937 се транспонира в България. Тя описва принципите управляващи системата за вътрешно докладване на дружеството и защитните мерки за докладващите лица.

2. Функциониране: Дружеството е установило система за вътрешно докладване предназначена за получаване и обработка на доклади/ сигнали относно нарушения на закона извършени от дружеството или член на персонала му, чрез канали за вътрешно докладване, т.е. специална електронна пощенска кутия и упълномощени лица, за получаване и обработка на доклади/ сигнали, сигурно и поверително.

Управителят клас А, Росен Русчев, е отговорен за внедряването на системата, а Диана Гимишева е назначена като системен мениджър, който изпълнява всички отговорности на служител обработващ доклади/ сигнали.

3. Персонален обхват (към кого се прилага): Политиката се прилага към всяко физическо лице, което има информация за нарушение извършено по време на минали или настоящи трудови взаимоотношения с дружеството, което е или е бил/а служител, работник или лице на заплатен труд, самонаето, безработно лице, занаятчия, или лице със свободна професия, заплатен или незаплатен доброволец или стажант, съдружник, акционер, едноличен собственик на капитала, член на ръководен или надзорен орган, член на одиторската комисия на предприятие, служител на наш изпълнител, подизпълнител, доставчик, кандидат за работа, който е запознат с нарушение в това си качество, наш работник или служител, който има информация за нарушение преди приключване на трудовите правоотношения, но който го докладва или оповестява публично на по-късен етап.

На всички тези лица и други, свързани с тях, се осигурява гаранция за защита на самоличността, поверителност, запазване в тайна на сигнализирането, и най-важното – защита срещу репресивни действия, за да се гарантира, че добросъвестно сигнализиране няма да доведе до уволнение на или отрицателно отношение и действия срещу докладващото лице.

4. Нарушения подлежащи на докладване/ сигнализиране: Каналите за вътрешно докладване са предназначени за получаване на доклади/ сигнали за действия или пропуски, които са в разрез със закона съгласно българското и законодателството на Европейския съюз, в сферите указани в

настоящата политика, или противоречат на обекта или целите на правилата в нормативните документи на Европейския съюз и сферите указани в настоящата политика. Политиката конкретизира видовете нарушения, които могат да бъдат докладвани/ сигнализирани.

Трябва да се отбележи, че тези вътрешни канали не са предназначени за получаване на оплаквания относно нарушение на етичните стандарти описани в Кодекса за бизнес поведение и други политики на групата Ретал. Поради някои правни и оперативни причини, включително необходимостта от спазване на строги правила при обработка на данни, дружеството създаде специални локални канали за обработка на тези специфични доклади.

Лицата изпращащи уместни доклади/ сигнали чрез каналите, съгласно правилата на политиката, подлежат на защита по закон.

5. Канали за докладване: Дружеството е установило следните канали за вътрешно докладване, а именно:

По електронен път:

whistleblower@retal.bg

По пощата:

РЕТАЛ БАЛКАН ЕООД
До: Мениджър на системата за
вътрешно докладване
Ул Керамика №13
Сливен 8800
България

Лично:

Мениджър система за вътрешно
докладване
Контакт на тел. +359 884 160 790
в рамките на работното време
за уговаряне на среща.

Ако даден доклад засяга мениджъра на системата за вътрешно докладване, указаният сигнал/доклад може да бъде предаден на Управител клас А, Росен Русчев, по пощенски път или лично, и ще бъде обработен съгласно политиката.

Всички колеги се насърчават да подават сигнали за загриженост или да докладват нарушения на закона в рамките на обхвата на политиката чрез някой от посочените канали.

Докладите НЕ МОГАТ да бъдат анонимни!

Доклади/ сигнали могат да се подават също към външни органи за властта.

Канал за външно докладване, България:

Комисия за защита на личните данни
Проф. Цветан Лазаров №2
София 1592
България
whistleblowing@cpdp.bg
Повече информация на: <https://www.cdpd.bg/>

Други канали за докладване/ сигнализиране в Европейския съюз

Доклади/ сигнали за нарушения на правото на Европейския съюз могат да бъдат подадени на:

https://commission.europa.eu/about-european-commission/contact/problems-and-complaints/complaints-about-breaches-eu-law/how-make-complaint-eu-level_es

6. Поверителност: докладващите и други защитени лица имат право тяхната самоличност да бъде запазена в тайна. Политиката гарантира, че се предприемат мерки за запазване на поверителността на данните.

7. Запазване в тайна: Информацията в системата остава поверителна и е достъпна единствено за оторизиран персонал. Изключения могат да се направят във връзка със спазването на законите.

8. Обработка на лични данни: Обработката на лични данни е в съответствие с изискванията на действащите разпоредби. Достъпът до лични данни е ограничен, данните се съхраняват за периода, за който е необходимо.

9. Забрана за репресия: Всяка форма на репресия е изрично забранена. Репресивните действия се третират като нарушения, подлежат на разследване и може да доведат до дисциплинарни действия.

10. Неспазване: Неспазването на политиката подлежи на разследване и може да доведе до прилагане на дисциплинарни мерки или други действия съгласно действащото законодателство.

Насърчаваме всеки служител да се запознае с политиката и да допринесе за установяването на култура на интегритет и отговорност в дружеството.

С уважение,

Росен Русчев
Управител клас А



Приета с решение на Управител клас А № 840 от 15.12.2023г.

РЕТАЛ БАЛКАН ЕООД
ПОЛИТИКА ЗА ВЪТРЕШНО ДОКЛАДВАНЕ

1. ЦЕЛ

- 1.1 Това е политика за вътрешно докладване („Политика“) възприета от РЕТАЛ БАЛКАН ЕООД („дружеството/ компанията“, „ние“, „нас“) очертаваща общите принципи на системата за вътрешно докладване и защитата на лицата, подаващи сигнали. Политиката следва Закона за защита на лицата, които подават сигнали или публично разкриват информация за нарушения, обнародван в Държавен вестник, брой 11 от 02.02.2023г., с поправките („Закон“).
- 1.2 Политиката описва начина на получаване и обработка на докладите/ сигналите за конкретни нарушения на закона, като използваме съществуващите си канали за вътрешно докладване.
- 1.3 Политиката осигурява гаранция за изчерпателност, интегритет и поверителност на информацията. Описва елементите на системата за вътрешно докладване и изискуемите по закон канали за предотвратяване на неоторизиран достъп до тази информация.

2. СИСТЕМА ЗА ВЪТРЕШНО ДОКЛАДВАНЕ. СТРУКТУРА И УПРАВЛЕНИЕ

- 2.1 Системата за вътрешно докладване („Система/та“) се състои от следните елементи:
- (1) Настоящата политика;
 - (2) Каналите за вътрешно докладване установени от дружеството;
 - (3) Ръководните структури на дружеството, системен мениджър, ролите и отговорностите им, както е описано в съответните политики;
 - (4) Наръчниците, разпоредбите и други документи одобрени от дружеството.
- 2.2 Управителят клас А на дружеството е отговорен за внедряването на системата.
- 2.3 Системата се управлява от лице или лица („Системен мениджър“) назначено/и от Управителя клас А, който изпълнява всички задължения на член на ръководството обработващ доклади. Системният мениджър може да изпълнява тази функция заедно с други задачи в дружеството, ако няма конфликт на интереси.
- 2.4 Всички или част от функциите на системата могат да бъдат делегирани на служители или членове на ръководството от други дружества. Това включва случаите, в които системният мениджър не може временно да изпълнява задълженията си, или ако докладът засяга системния мениджър, или лице свързано с него. Необходимите мерки трябва да бъдат

предприемани постоянно, за да се осигури съответствие на такива делегирани функции с принципите и гаранциите постановени в настоящата политика.

- 2.5 Системният мениджър или негов представител/ делегат, според случая, трябва да работи независимо от останалата част от дружеството. Никой не може да инструктира системният мениджър или такъв представител, да изпълнява функция, която му е възложена.
- 2.6 Можем да възложим получаването на доклади/ сигнали на друго физическо или юридическо лице, в съответствие със закона.

3. ПЕРСОНАЛЕН ОБХВАТ

- 3.1 Настоящата политика се прилага по отношение на всяко физическо лице (всяко „**докладващо/ сигнализиращо лице**“), което е имало информация за нарушение по време на работните взаимоотношения с нас, както в миналото, така и понастоящем, и който/която е бил/а или е:
 - (1) Наш работник, служител, или друго лице, което е на заплатен труд при нас;
 - (2) Самонает, безработен, занаятчия, или лице със свободна професия;
 - (3) Доброволец или стажант, работещ със или без заплащане.
 - (4) Партньор, акционер, едноличен собственик на капитала, член на управителен или надзорен орган, член на одиторската комисия на предприятие;
 - (5) Служител на наш изпълнител, подизпълнител или доставчик;
 - (6) Кандидат за работа, който има информация за нарушение в това си качество;
 - (7) Наш работник или служител, който има информация за нарушение преди приключване на трудовото си правоотношение, но който го сигнализира или оповестява публично по-късно; или
- 3.2 Доклади/ сигнали от всяка друга категория лица, невяклучени в т. 3.1. по-горе, са изрично изклучени от обхвата на тази политика.
- 3.3 Тази политика също защитава всяко физическо лице, което:
 - (1) Подпомага докладващото лице при сигнализирането на нарушения по смисъла на Закона за защита на лицата, които подават сигнали или публично разкриват информация за нарушения при условие за поверителност;
 - (2) Е свързано с докладващото лице по служебна или роднинска линия, и което може да бъде подложено на репресия в резултат на докладването; или
 - (3) Публично разкрие информация относно нарушение.
- 3.4 Правната защита в допълнение обхваща юридическите лица, в които докладващото лице притежава дял, работи там или по друг начин е свързано служебно с юридическото лице.

4. ИНФОРМИРАНOST

Настоящата политика трябва да бъде предоставена на служителите на дружеството, изложена в помещенията му, да бъде налична в електронната интранет система с ресурси на разположение на служителите на дружеството на <https://retalcorp.sharepoint.com>, и също така може да бъде публикувана чрез други източници.

5. НАРУШЕНИЯ ПОДЛЕЖАЩИ НА ДОКЛАДВАНЕ

5.1 Каналите за вътрешно докладване са създадени за получаване на сигнали (всеки наричан „Доклад/сигнал“ или „Доклади/ сигнали“) по действия или пропуски, които са незаконни и свързани с българското законодателство или документи на Европейския съюз, в областите свързани с тази политика (наричани „нарушение“):

- (1) Нарушения на българските закони или законите изброени в анекса към Директива (ЕС) 2019/1937 на Европейския парламент и Съвета, от 23.10.2019г. относно защитата на лица, които подават сигнали за нарушения на правото на Съюза в следните сфери:
 - (i) Обществени поръчки;
 - (ii) Финансови услуги, продукти и пазари, и превенция на изпирането на пари и финансиране на тероризъм;
 - (iii) Безопасност на продуктите и съответствие;
 - (iv) Безопасност на транспорта;
 - (v) Защита на околната среда;
 - (vi) Защита от радиация и ядрена безопасност;
 - (vii) Безопасност на храните и фуражите, здравето и благополучието на животните;
 - (viii) Обществено здраве;
 - (ix) Защита на потребителя;
 - (x) Защита и поверителност на личните данни;
 - (xi) Сигурност на мрежата и информационните системи;

- (xii) Защита на финансовите интереси на Европейския съюз както е постановено в чл. 325 от Договора за функционирането на Европейския съюз (TFEU);
 - (xiii) Вътрешния пазар, както е указано в чл. 26(2) от Договора за функционирането на Европейския съюз, включително защита на икономическата конкуренция и държавното финансиране съгласно правото на Европейския съюз.
- (2) Нарушения свързани с трансгранични данъчни схеми, с цел получаване на данъчни привилегии, което противоречи на целите на действащото законодателство в областта на корпоративното облагане;
- (3) Престъпления от общ характер известни на сигнализиращото лице във връзка с работата му/й; или
- (4) Нарушения на българските закони в следните области:
 - (i) Публични финанси, или местни данъци;
 - (ii) Труд;
 - (iii) Обществени услуги.
- 5.2 Минали нарушения, които са извършени две години преди сигнализирането или по-рано, не попадат в обхвата на настоящата политика.
- 5.3 Каналите за вътрешно докладване не трябва да се използват за оплаквания относно:
 - (1) Междудличностни конфликти;
 - (2) Нарушения, които не влизат в обхвата на настоящата политика;
 - (3) Неудовлетвореност на наш клиент; или
 - (4) Въпроси извън служебния контекст.
- 5.4 Въпросите указани в точка 5.3 по-горе са извън обхвата на настоящата политика. На всяко сигнализиращо лице, чийто доклад засяга такъв въпрос трябва да бъде предоставена възможност и насоки за корекция на нередността в доклада в рамките на седем дни от получаването му. Доклад, който не е коригиран в този срок не трябва да бъде обработван, а да бъде върнат на сигнализиращото лице заедно с всички приложения.

6. ИНФОРМАЦИОННИ КАНАЛИ

Канали за вътрешно докладване

- 6.1 Дружеството е установило няколко канала за докладване. Ако сигнализиращото лице има основания да смята, че информацията за дадено нарушение е вярна и то влиза в обхвата на настоящата политика, такова лице се насърчава да докладва незабавно.
- 6.2 Такъв доклад може да бъде направен чрез няколко от следните средства:
- (1) По електронен път (имейл) на: whistleblower@retal.bg;
 - (2) По пощата на следния адрес:

РЕТАЛ БАЛКАН ЕООД
На вниманието на: Системен мениджър по вътрешно докладване
Ул. Керамика №13
Сливен 8800
България;
или
 - (3) лично.
- По искане на сигнализиращото лице, докладът може да бъде направен устно лично пред системния мениджър. Уреждане на лична среща може да стане чрез указаните канали или като се свърже директно със системния мениджър. Системният мениджър трябва да организира лична среща в рамките на разумен срок от получаването на искането.
- 6.3 Доклади, отнасящи се **до системния мениджър** се получават лично от Управител клас А, по пощата, изпратени на адреса на дружеството или чрез лична среща.
- 6.4 Всяко лице, с изключение на лицата упълномощени да получават доклади съгласно политиката, което получи доклад, трябва незабавно да го препрати чрез предназначения за това информационни канали до системния мениджър. Трябва да се полагат грижи при изпращането за защита на личните данни и поверителността на съдържанието на доклада. Нарушение на това изискване трябва да бъде разследвано и може да доведе до възникване и ангажиране на дисциплинарна отговорност на виновното/виновните лице/лица, ако това нарушение не подлежи на по-тежко наказание, предвидено от законите.
- 6.5 Като приоритет, всеки доклад трябва да бъде подаден чрез канал за вътрешно докладване, освен ако има риск за сигнализиращото лице от репресия, дискриминация или че няма да бъдат предприети ефективни мерки.
- 6.6 И все пак дадено нарушение може да бъде докладвано и отвън. Външен доклад трябва да бъде изпратен вместо, успоредно с, или след вътрешен сигнал. На лица, които желаят да подадат сигнал трябва да бъде предоставена ясна и леснодостъпна информация относно процедурите за външно докладване до компетентните централни власти и, ако е приложимо, до институции, органи, служби и агенции на Европейския съюз.
- 6.7 **Канал за външно докладване в България**

Комисия за защита на личните данни

Писмено:

По електронен път на: whistleblowing@cpdp.bg.

По пощата:

Проф. Цветан Лазаров № 2

София 1592

България

Устно: на място в Комисията в София 1592, Проф. Цветан Лазаров № 2.

Повече информация на: <https://www.cdpd.bg/>

Други канали за докладване в Европейския съюз

Доклади относно нарушения на правото на Европейския съюз трябва да бъдат подавани на:

https://commission.europa.eu/about-european-commission/contact/problems-and-complaints/complaints-about-breaches-eu-law/how-make-complaint-eu-level_es

7. ФУНКЦИОНИРАНЕ

7.1 Получаване на доклади

- (1) Писмените доклади трябва да се подават чрез попълване на стандартен [образец](#), одобрен от Комисията за защита на личните данни, или неин правоприемник, като централен орган за външно докладване съгласно законите ("комисия"). Такива доклади могат да бъдат изпращани по пощенски път, имейл, или предавани лично на системния мениджър.
- (2) Без значение как е изготвен, докладът трябва да включва информация, която:
 - (i) Ни позволява да идентифицираме сигнализиращото лице, и
 - (ii) Конкретизира извършеното нарушение с давност не повече от две години.
- (3) За да е в съответствие с параграф (2) по-горе, докладът трябва да включва, минимум следната информация:
 - (i) Името, адресът и телефонният номер на изпращача, както и електронният адрес, ако има такъв;
 - (ii) Името на лицето срещу което докладът се подава и работното му място, ако докладът обвинява конкретно познато лице;
 - (iii) Конкретна информация относно извършеното докладвано нарушение, не повече от две години преди това, и реалната вреда, която причинява,

място и период на извършване, ако даденото нарушение е извършено, описание на действието или ситуацията и други обстоятелства, доколкото те са известни на докладващото лице;

- (iv) Дата на изпращане на доклада; и
 - (v) Подпис, електронен подпис, или друга идентификация на изпращача.
- (4) Насърчава се докладващото лице да включи в доклада всякакви източници на информация, които могат да потвърдят докладваното и/или да се позове на документи, които могат да бъдат приложени към доклада, включително указване на лица, които могат да потвърдят докладваното или да предоставят повече информация.
- (5) Доклади при лична среща трябва да бъдат документирани чрез подаване на стандартен образец, одобрен от Комисията. На сигнализиращото лице трябва да бъде предложена възможност за проверка, корекция, и да потвърди образца чрез подпис. Преди проверката, докладващото лице трябва да бъде информирано, че данните му/и ще бъдат обработени в съответствие с Регламент (ЕС) 2016/679, с транспозицията му в законодателството на България. Личната среща с докладващо лице трябва да бъде проведена в сградата или друго място, което защитава самоличността на сигнализиращото лице.
- (6) Системният мениджър носи отговорност да организира получаването на докладите, както е описано в точка 7.1 (Получаване на доклади). Системният мениджър може да делегира тази отговорност на лице, посочено от дружеството, особено когато докладът засяга системния мениджър или свързано с него/нея лице. Делегатът може да бъде външно физическо или юридическо лице. В момента на назначаване на делегата на тази длъжност, той/тя поема задълженията на системния мениджър описани в тази политика и закона, до степената на делегираните отговорности.

7.2 Регистрация на доклади и предоставяне на статистическа информация

- (1) Информация за всеки получен доклад, попадащ в обхвата на тази политика и закона, трябва своевременно да бъде вписана в регистъра поддържан съгласно настоящата политика, дори ако докладът:
- (i) Е свързан с нарушение извършено преди повече от две години;
 - (ii) Е свързан с неправдоподобни факти;
 - (iii) Е свързан с нарушение, което подлежи на докладване по друг закон или разпоредба;

- (iv) Не съдържа нова или значима информация относно вече докладвано нарушение, или
 - (v) Е анонимен, но сигнализиращото лице е идентифицирано на по-късен етап и е станало обект на репресия.
- (2) За регистрацията на доклад, който не е анонимен, използваме уникален идентификационен номер **(УИН)**, генериран от Комисията и подаван към нас за всеки доклад.
 - (3) Ако сигнализиращо лице подаде доклад в писмена форма, различна от одобрената от комисията, системният мениджър или друго упълномощено лице трябва да въведе информацията от доклада в одобрената от Комисията форма, без да копира, пре(на)писва, разказва или по друг начин възпроизвежда доклада.
 - (4) Липса на изисквана информация, по параграф (ii) от точка 7.1 (Получаване на доклади) не е причина за нерегистриране на доклада.
 - (5) Само доклади свързани с въпроси указани в т. 5.3 на настоящата политика не трябва да се регистрират.
 - (6) Необходимо е всяка година, преди 31-ви януари, да предоставяме на Комисията статистическа информация, която включва броя на получените доклади, идентификационните им номера, предмета, броя на извършените разследвания и резултатите от тях.
 - (7) Системният мениджър е отговорен за съхранението и поддръжката на регистъра описан в т. 7.2 (Регистрация на доклади и статистика). Системният мениджър може да делегира тази отговорност на лице, назначено от дружеството на тази длъжност, особено когато докладът засяга системния мениджър или свързано с него/нея лице. Пълномощникът трябва да бъде служител или член на ръководството на дружеството, който е функционално независим и незасегнат от конфликт на интереси. В допълнение, лицето с възложена функцията описана в параграф (6) по-горе, трябва да бъде оторизирано от дружеството да оценява и разследва докладите, които да се включат в годишния статистически доклад. В момента на назначаване на делегата на тази длъжност, той/тя поема задълженията и отговорностите на системния мениджър описани в настоящата политика и закона, до степента на делегираните функции.

7.3 Потвърждение за получаване на доклади

- (1) При възможност, получаването на доклада трябва да бъде потвърдено в писмен вид на сигнализиращото лице в рамките на няколко календарни дни от получаването му.
- (2) Потвърждението по параграф (1) не трябва да бъде изпращано ако:

- (i) Докладващото лице не е предоставило адреса си;
 - (ii) Докладът е анонимен; или
 - (iii) Може пряко или косвено да разкрие самоличността на сигнализиращото лице или да създаде предположение за неговата самоличност.
- (3) Ведно с потвърждението по параграф (1), докладващото лице трябва да получи и уникален идентификационен номер и входящ номер на доклада.

7.4 Оценка на доклади

- (1) Ако докладът е изчерпателен и уместен, ще бъде оценен, включително това дали попада в обхвата на настоящата политика.
- (2) Ако информацията е недостатъчна, от докладващото лице трябва да бъде поискана допълнителна информация. На всяко сигнализиращо лице, чийто доклад съдържа несъответствията описани в подпараграф (i) от параграф (3) по-долу, трябва да бъде предоставена възможност и насоки за корекция в рамките на седем дни от получаването му. Ако докладът не бъде коригиран в рамките на този срок, не трябва да бъде обработван повече и да бъде върнат на докладващото лице ведно с всички приложения.
- (3) При внимателен анализ на доклада, трябва да бъде взето едно от следните решения:
 - (i) Освен ако докладът не бъде коригиран в рамките на срока по параграф (2) по-горе, случаят се приключва като недопустим без разследване, при наличие на следните причини:
 - (1) Представените факти в доклада не са потвърдени;
 - (2) Докладваните факти не представляват нарушение влизащо в обхвата на политиката;
 - (3) В доклада липсва информацията изискуема по параграф (ii) на т. 7.1 **Error! Reference source not found.** (Получаване на доклади); или
 - (4) Докладът е подаден от лице, което не попада в обхвата на действие на настоящата политика;
 - (5) Наличие на други причини за приключване на случая без разследване съгласно законите и настоящата политика;

- (ii) Организиране на последващи действия във връзка с доклада, за която цел може да поискат съдействие от други лица или отдели на дружеството – за разследване на доклада;
- (iii) Предложение до ръководството на дружеството да предприеме конкретни мерки, за да спре или предотврати нарушението, при установяване на такова нарушение или когато има реален риск за предстоящо извършване;
- (iv) Да насочи докладващото лице към съответния правоприлагащ/правораздавателен или регулаторен орган, когато правата на сигнализиращото лице са засегнати;
- (v) Да препрати доклада до Комисията ако:
 - (1) Ако докладът дава основание за предприемане на действия от Комисията; и
 - (2) Докладващото лице е информирано за препращането предварително;и/или
- (vi) Да се насочи докладващото лице да сигнализира Комисията, ако докладът се подава срещу работодателя на докладващото лице.
- (vii) Да препрати доклада до Комисията в рамките на седем дни, заедно с цялата първоначално и/или последващо събрана документация към него и без заличаване на данни, ако докладът:
 - (1) Идва от работодател в частния сектор, за който не се изисква да спази процедурата за каналите на вътрешно докладване съгласно закона;
 - (2) Свързано е с нарушение извършено от лице на висока обществена длъжност съгласно чл. 6 от Закона за борба против корупцията и отнемане на незаконно придобито имущество;
 - (3) Свързано е с дейност или друга задължена организация съгласно закона без да идентифицира юридическото лице;
 - (4) Изисква предприемане на действия от страна на Комисията съгласно закона; или
 - (5) След като е регистриран от системния мениджър, е отишъл директно до някоя от публичните институции указани в закона;

- (4) Комуникацията до властите трябва да бъде направена при условие, че не нарушава законността или основните права на физическите и/или юридически лица, които биха могли да бъдат засегнати от въпросните факти.

7.5 **Обработка на докладите. Разследване.**

- (1) Ще положим усилия да разследваме всеки допустим доклад.
- (2) Системният мениджър организира разследването като изисква, при необходимост, съдействието на други служители или отдели на дружеството.
- (3) Разследващите не трябва да имат личен интерес (субективност) относно резултатите на разследването. Разследващ, който има личен интерес, трябва да се въздържа от участие в разследването и да докладва този факт на лицето, което оторизира разследването веднага щом установят, че имат личен интерес.
- (4) При всяко разследване на доклад, трябва да следваме съответно предписаната от закона процедура. То (разследването) трябва да цели обективна и достоверна оценка на фактите във всичките им аспекти и в целостта им. Търсят се всички нарушения, които влизат в обхвата на настоящата политика, и всички лица отговорни за тях. Също трябва да се идентифицират лицата, които са съдействали и/или облагодетелствали от тях.
- (5) Разследващият трябва да има достъп до документите и информацията на дружеството, да посещава помещенията, да се среща със служителите, включително в поверителни срещи.
- (6) Подаването на външен доклад не е причина за спиране на разследването по доклада.
- (7) Разследването приключва с индивидуален доклад, на вниманието на лицето, което го е оторизирало.
- (8) Максималният период на разследване на сигнализиран проблем не може да превишава три месеца. Периодът започва със споменатото по-рано потвърждение на получаването на доклада, ако има такова, или от изтичането на седмодневен срок, считано от датата на подаване на сигнала.

7.6 **Изход от разследването**

- (1) При установяване на нарушение, дружеството трябва:
 - (i) Да приключи случая ако:
 - (1) Докладваното нарушение е незначително и не изисква допълнителни последващи действия;

- (2) Докладът не съдържа нова или съществена информация относно нарушение в сравнение с обработени предходни приключени доклади; или
 - (3) Установено е доказателство за престъпление и докладът заедно с прилежащите материали е нужно да бъде изпратен незабавно до прокуратурата;
 - (ii) На базата на доклада и предложението на системния мениджър, се предприемат подходящи мерки за спирането или превенция на нарушението;
 - (iii) След установяване на самоличността на докладващото лице, за което са взети мерки за защита, се подготви индивидуален доклад, който трябва:
 - (1) Накратко да описва информацията от доклада, предприетите действия, крайния резултат от проверката или разследването на доклада;
 - (2) Да бъде, ведно с основанията, изпратен на нашият работник или служител, който е подал доклада и на засегнатото лице; и/или
 - (iv) Да се препрати информация до съответните власти, съобразно тяхната компетентност.
- (2) Когато случаят е приключен на основанията указани в раздели (1) (i) (1) и (2) на т. 7.6 (Изход от разследването), докладващото лице може да подаде доклад до Комисията.
 - (3) Нарушенията може да изискват прилагането на дисциплинарни мерки срещу засегнатото лице. Такива мерки трябва да са в съответствие със законите, разпоредбите и корпоративните политики.
 - (4) Лицето подало фалшив доклад също подлежи на прилагане на дисциплинарни мерки.

7.7. Обратна връзка/ информация

На докладващото лице и засегнатото от доклада лице трябва да бъде предоставена информация относно планираните действия или последващо предприетите мерки, както и основанията за тях, както се изисква в параграф (1) от т. 7.6 (Изход от разследването).

8. ПОВЕРИТЕЛНОСТ

- 8.1 Всяко лице подало доклад/ сигнал има право нейната/неговата самоличност да не бъдат разкривани на трети страни. Освен ако не се изисква по закон или за това има изрично писмено съгласие, ние няма да разкриваме самоличността на докладващото лице, на

лицето засегнато от (обект на) доклада, или всяко друго лице указано в доклада, на никой, който не е необходимо да знае, за да бъде обработен докладът.

- 8.2 За да се защити самоличността на замесените лица, ще предприемем мерки да пазим техните данни конфиденциални, особено тези на докладващото лице.
- 8.3 Може по закон да се изиска от нас да разкрием самоличността на докладващото лице на обществен орган/институция. Преди такова разкриване, ние трябва:
- (1) Да информираме докладващото лице относно необходимостта за разкриване;
 - (2) Да му предоставим причините/ основанията, на които предоставяме тази информация за самоличността му; и
 - (3) Да му се позволи да коментира относно предоставянето на тази информация на обществени органи.
- 8.4 Уведомлението по т. 8.3 трябва да бъде в писмен вид. Такова уведомление не трябва да се изпраща, ако може да попречи на разследването на националните власти, съдебни процеси или производства.
- 8.5 Засегнатото от доклада лице при никакви обстоятелства не трябва да има информация относно самоличността на докладващото лице.

9. ЗАПАЗВАНЕ В ТАЙНА

- 9.1 Информацията документирана в системата остава поверителна. Това включва съдържанието и детайли на доклада, потвърждение, оценка, разследване, заключение, и обратна информация. Понякога тази информация сме задължени да споделим за целите на разследване, действия или спазване на закона.
- 9.2 Само оторизирани служители могат да имат достъп до системата. В изключителни случаи, може да бъде споделена с трети страни, при изискване по закон, с подходящите предпазни мерки.

10. ОБРАБОТКА НА ЛИЧНИ ДАННИ

Обработката на лични данни съгласно тази политика трябва да бъде в съответствие с принципите и правилата предвидени в законите за защита на лични данни и действащите корпоративни правила. **Приложение 1 съдържа информация за защитата на лични данни и упражняването на права.**

ЗАБРАНА ЗА РЕПРЕСИВНИ ДЕЙСТВИЯ

- 11.1 Изрично забраняваме всякаква форма на репресия. Това включва действия или пропуски, неразрешени от закона, или такива, които пряко или косвено включват отрицателно

отношение, което поставя потърпевшите в особено неблагоприятно положение в трудов или професионален контекст единствено поради техния статут на докладващо лице, или защото са направили публично оповестяване.

- 11.2 Третираме репресията сама по себе си като нарушение. Ще положим усилия да разследваме всяко репресивно действие надлежно. Извършителят на такива репресивни действия може да бъде подложен на дисциплинарни или други съответни мерки, съгласно изискванията на закона.
- 11.3 Всяко докладващо лице, което стане обект на репресивно отношение трябва да сигнализира чрез някой от каналите за вътрешно докладване.

11. ЗАЩИТА НА ЗАСЕГНАТИТЕ ЛИЦА

12.1 Лицата засегнати от доклада ("**засегнати лица**") имат следните права:

- (1) Да получат защита на разкриване на самоличността им пред лица, които не е нужно да ги познават, за да обработят доклада съгласно тази политика, освен ако такова разкриване не се изисква по закон или е изрично заявено писмено;
- (2) Да защитят себе си, да бъдат изслушани, да дадат писмени обяснения, да предоставят доказателства по време на процеса на оценка и разследване на доклада/ите, който/които ги уличава/т;
- (3) Да им се осигури информация за всички събрани срещу тях доказателства и да им се предостави възможност да подадат възражение срещу доклада в рамките на седем дни; и
- (4) Да им се даде възможност да предоставят нови доказателства в процеса на разследване.

12.2 При комуникация със засегнатото лице, не може пряко или косвено да се разкрива самоличността на докладващото лице или да се създава предположение за нея.

12. СЪХРАНЕНИЕ НА АРХИВ

13.1. След получаване на доклада, като минимум, следната информация указана в [образеца](#), одобрен от Комисията трябва да бъде въведена в регистъра ("**регистър**"):

- (1) Лицето получило доклада;
- (2) Дата на подаване на доклада;
- (3) Засегнатото лице, ако такава информация присъства в доклада;

- (4) Резюме на предполагаемото нарушение, като място и период на извършване на нарушението, описание на действието и други обстоятелства при които е извършено;
- (5) Връзката на подадения доклад с други установени доклади при обработката му;
- (6) Обратната информация подадена към сигнализиращия и датата на предоставяне;
- (7) Предприети последващи действия;
- (8) Резултати от оценката и/или разследването на доклада;
- (9) Периодът на съхранение на доклада;
- (10) Нашият входящ регистрационен номер;
- (11) Уникалният идентификационен номер.

13.2. Регистърът не трябва да е публичен. Достъп до регистъра може да има само:

- (1) Системният мениджър или лицето изпълняващо тяхната длъжност;
- (2) Комисията и служителите ѝ; и
- (3) Служителите на дружеството, които трябва да имат достъп до регистъра, за да предприемат последващи действия или да предотвратят нарушение, без да се разкрива самоличността на докладващото или засегнатото лице.

13.3. Докладът и свързаната с него документация, включително лични данни съдържащи се в него, трябва да бъдат съхранявани на защитен, траен и достъпен носител. Трябва да бъдат съхранявани само за необходимото време, за обработка на доклада, и във всички случаи не повече от пет години от датата на приключване на обработката на доклада, освен ако във връзка с него не продължават наказателни, граждански производства, свързани с трудовото законодателство и/или административни производства.

13. НЕСПАЗВАНЕ

Неспазването на политиката трябва да се разследва и може да предизвика прилагането на дисциплинарни мерки и/или отговорност, съгласно действащото законодателство.

РЕТАЛ БАЛКАН ЕООД**ПОЛИТИКА НА ВЪТРЕШНО ДОКЛАДВАНЕ**

Приложение1

Информация за защитата на лични данни и упражняване на права

Информация с препратка в чл. 13 на Регламент (ЕС) 2016/679 на Европейския парламент и Съвета, от 27.04. 2016г.

(“Регламент (ЕС) 2016/679”)

Самоличността и данните за контакт на администратора и, където е приложимо, пълномощник на администратора:	РЕТАЛ БАЛКАН ЕООД Ул. Керамика №13 Сливен 8800 България тел. +35944681188 електронен адрес: bulgaria@retalgroup.com
Данните за контакт на служителя за защита на личните данни, където е приложимо:	Неприложимо.
Целите на обработка, за които личните данни са предназначени, както и правното основание за обработката:	Цели на обработка: събиране и обработка на информация за нарушения. Правно основание за обработка: чл. 6.1. (а), (в), (д) от Регламент (ЕС) 2016/679.
Където обработката е основана на т. (е) от чл. 6(1)на Регламент (ЕС) 2016/679, законният интересследван от администратора или от трета страна:	Неприложимо.
Реципиентите или категориите от реципиенти на лични данни, ако има такива:	Администратори на данни, обществени органи, агенция, или друга служба, на която личните данни се разкриват съгласно действащото законодателство, лица извършващи разследване на докладите и прилагане на съответните мерки.
Фактът, че администраторът на данни възнамерява да прехвърли лични данни към трета държава или международна организация, и съществуването или липсата на решение за	Лични данни могат да бъдат прехвърлени на трета държава – член на Европейския съюз, Великобритания или друга държава, или

адекватност от Комисията, или в случай на трансфер съгласно чл. 46 или 47 или вторият параграф на чл. 49(1), Регламент (ЕС) 2016/679 относно разумните/уместните предпазни мерки и средствата, с които да се получи копие от тях, или къде са достъпни:	международна организация, при спазване на разпоредбите на Регламент (ЕС) 2016/679.
Периодът, за който личните данни ще бъдат съхранявани, или ако това не е възможно, критериите използвани за определяне на този период:	Данните ще бъдат съхранявани за период необходим за спазване на разпоредбите на Закона за защита на лица, които подават сигнали или разкриват публично информация за нарушения, №11 от 02.02.2023г. Данните не трябва да бъдат съхранявани за период по-дълъг от пет години.
Съществуването на право на заявяване към администратора на достъп до и корекция или заличаване на лични данни, или рестрикция за обработка относно субект на данни или внасяне на възражение срещу обработка, както и право на пренос на данни:	Имате право да изискате от администратора достъп до и корекция, или заличаване на лични данни, или рестрикция за обработка относно субекта на данни, или да подадете възражение срещу обработката, както и право на пренос на данни.
В случаите когато обработката се основава на точка (а) от чл. 6(1) или т. (а) от чл. 9(2) на Регламент (ЕС) 2016/679, съществуването на право за оттегляне на съгласие по всяко време, без да се засегне законността на обработката на базата на съгласието преди оттеглянето му:	В рамките на данните обработени по точка (а) от чл. 6(1) или т. (а) от чл. 9(2) на Регламент (ЕС) 2016/679, имате право да оттеглите съгласието си по всяко време, без това да засегне законността на обработката на база съгласие дадено преди оттеглянето му.
Право на подаване на оплакване/жалба в надзорен орган:	Имате право да подадете жалба/оплакване в надзорен орган: Комисия за защита на личните данни Бул. Проф. Цветан Лазаров №2 София 1592 България Електронен адрес: kzld@cpdp.bg
Дали предоставянето на лични данни е законово или договорно изискване, или изискване	Предоставянето на лични данни е изискуемо за правилното получаване и обработка на доклада

необходимо за сключване на договор, както и дали субектът на данни е задължен да предостави лични данни и възможните последиствия от непредоставянето им:	съгласно Закона за защита на лица, които подават сигнали или публично разкриват информация за нарушения, №11 от 02.02.2023г.
Упражняването на автоматично вземане на решения, включително профилиране, както е указано в чл. 22(1) и (4) на Регламент (ЕС) 2016/679и, поне в тези случаи, смислена информация относно логиката, както и значението на предвидените последиствия от такава обработка за субекта на данни:	Автоматично вземане на решения не съществува.
Възможност за упражняване на правата предвидени в чл. 15 до 22 от Регламент (ЕС) 2016/679:	Имате право на достъп за корекция, заличаване, рестрикция на обработката, на възражение срещу индивидуално автоматично вземане на решения, както и на право да не бъдете обект на решение единствено на базата на автоматична обработка, което може да се упражнява до степента и по реда предвиден в Регламент (ЕС) 2016/679.