

## **Насоки за сигнализиране за нередности на Embracer Group**

Прието от ръководителя на „Персонал, правни и управленски въпроси“ на Embracer Group на 12 септември 2023 г.

Ревизиран:

Вид на документа: Насоки

Версия: 1

Собственик на документа: Ръководител на отдела за управление и съответствие на Embracer Group

Настоящите насоки се прилагат за дружествата на Embracer Group и за всички служители в Embracer Group.

Тези насоки разширяват и подробно описват рутината и инструментите за сигнализиране за нередности в рамките на Embracer Group. Успоредно с тези насоки могат да съществуват насоки на местно ниво, за да допълнят местните правни изисквания или процеси.

Ако имате някакви въпроси относно тези насоки, моля, свържете се с:  
Ръководител на отдела за управление и съответствие на Embracer Group, правни

**Насоки за сигнализиране за нередности на Embracer Group**

**Съдържание**

1.	История на редакциите .....	3
2.	Въведение - какво е подаване на сигнали и защо е важно? .....	3
3.	Кога да подадете сигнала? .....	4
4.	Как да подадете сигнала? .....	5
5.	Процесът на разследване .....	6
6.	Защита и поверителност .....	8
7.	Приложения .....	10

## 1. История на редакциите

Дата	Версия	Описание	Автор
09-12-2023 г.	1.0	Първа версия, приета от ръководителя на „Персонал, правна и управленска дейност“ на Embracer Group	Ръководител „Управление и съответствие“

## 2. Въведение - какво е подаване на сигнали и защо е важно?

- 2.1 Нашата организация се стреми към постигане на прозрачност и високо ниво на бизнес етика. Embracer Group AB и нейните дружества („Embracer Group“) имат нулева толерантност към действия като дискриминация, тормоз, престъпност, корупция и екологични престъпления. Равното третиране на всички служители в Embracer Group („Служителите“), клиентите и доставчиците, както и добрата бизнес етика, са ключов елемент. Тези основни ценности са документирани в нашия Кодекс за поведение и нашия Кодекс за поведение на доставчиците. Кодексите описват принципите и подхода на Embracer Group за служителите и бизнес партньорите, както и за Embracer Group като работодател и член на общността.
- 2.2 Embracer Group насърчава своите служители, бизнес партньори, доставчици и други външни контакти да уведомят Embracer Group/ организацията, ако са установили сериозен проблем или имат сериозни подозрения за измама, корупция, тормоз или други подобни нередности в рамките на дейността на Групата. Служителите, а също и трети страни, имат важна роля при уведомяването, ако подозират нещо, което противоречи на Кодекса за поведение на Embracer Group/ Кодекса за поведение на доставчиците. Това дава възможност на Embracer Group/ организацията не само да предотврати, но и да коригира, ако нещо се е объркало. Нашата услуга за подаване на сигнали за нередности предлага възможност за уведомяване на Embracer Group/ организацията за подозрения за неправомерно поведение по поверителен начин. Това е важен инструмент за намаляване на рисковете и поддържане на доверие в нашите операции, като ни позволява да откриваме и действваме при евентуално неправомерно поведение на ранен етап. Подаването на сигнали за нередности може да се извършва от всяко лице открито или анонимно.
- 2.3 Целта на настоящите насоки е отчасти да информираме за нашите вътрешни канали за докладване и как се извършва докладването и проследяването на докладите, а отчасти да гарантираме, че изпълняваме задълженията си съгласно Директива [ЕС] 2019/1937 на Европейския парламент и на Съвета относно защитата на лицата, които съобщават за нарушения на правото на Съюза и приложимите правила за защита на

данните („Директивата за сигнализиране за нередности“), както и всички специфични местни изисквания в държавите-членки на ЕС, в които работим. Настоящите насоки се прилагат за всички служители, изпълнители, стажанти, кандидати за работа и други лица, които извършват или са извършвали работа за и под ръководството на Embracer Group в Европейския съюз.

### **3. Кога да подадете сигнала?**

- 3.1 Услугата за подаване на сигнали за нередности може да се използва за докладване на нарушения, попадащи в следните области („Зоните на обхват“), които са:
1. Нарушения на правото на Европейския съюз, попадащи в съществения обхват на Директивата за сигнализиране за нередности, включително:
    - Нарушения, попадащи в обхвата на актовете на Съюза, посочени в приложението към Директивата за сигнализиране за нередности, които засягат следните области:
      - Обществени поръчки;
      - Финансови услуги, продукти и пазари, както и предотвратяване на изпирането на пари и финансирането на тероризма;
      - Безопасност и съответствие на продуктите;
      - Безопасност на транспорта;
      - Опазване на околната среда;
      - Радиационна защита и ядрена безопасност;
      - Безопасност на храните и фуражите, здравето и хуманното отношение към животните;
      - Обществено здраве;
      - Защита на потребителите;
      - Защита на неприкосновеността на личния живот и личните данни и сигурността на мрежовите и информационните системи.
    - Нарушения, засягащи финансовите интереси на Европейския съюз, както е посочено в член 325 от ДФЕС и както е допълнително уточнено в съответните мерки на Съюза; както и
    - Нарушения, свързани с вътрешния пазар, посочени в член 26, параграф 2 от ДФЕС, включително нарушения на правилата на Съюза за конкуренцията и държавните помощи, както и нарушения, свързани с вътрешния пазар във връзка с действия, които нарушават правилата за корпоративното данъчно облагане или договорености, чиято цел е да се получи данъчно предимство, което противоречи на предмета или целта на приложимото законодателство за корпоративното данъчно облагане.
  2. Всяко друго нарушение в областите, предписани от националното законодателство, както е изброено по-нататък в съответните специфични за държавата приложения по-долу.

- 3.2 Служителите са помолени да се свържат със своя ръководител „Човешки ресурси“, мениджър или местен служител за съответствие или функция по въпроси, свързани с недоволството на работното място или свързаните с тях въпроси, тъй като тези въпроси не могат да бъдат разследвани в обхвата на подаването на сигнали за нередности.
- 3.3 Човек, който подава сигнал, не трябва да има твърди доказателства за изразяване на подозрение. Умишленото съобщаване на невярна или злонамерена информация, обаче, е забранено. Злоупотребата със службата за подаване на сигнали за нередности може да представлява дисциплинарно нарушение, което може да доведе до дисциплинарни действия до прекратяване, предмет на местното законодателство.
- 3.4 Моля, имайте предвид, че обхватът на нарушенията, за които се съобщава, може да бъде по-широк в някои държави и че може да има специфични разпоредби и изисквания за използването на услугата за сигнализиране за нередности. Моля, вижте повече информация на адрес: <https://report.whistleb.com/embracer> — където при избора на вашия език ще бъдат показани специфични разпоредби за отделните държави и в специфичните за държавата приложения към тези насоки, **Приложения А -О.**

#### 4. Как да подадете сигнала?

- 4.1 Има различни начини да изразите загриженост:
- **Алтернатива 1:** Свържете се с ръководител „Човешки ресурси“, мениджър или местен служител по съответствие или функция в рамките на нашата организация.
  - **Алтернатива 2:** Контакт:  
Embracer Group AB, ръководител на „Персонал, правна и управленска дейност“, Иън Гулам  
Телефон: +46 72 857 70 17 Имейл: [ian.gulam@embracer.com](mailto:ian.gulam@embracer.com)  
Доклад може да бъде направен и чрез физическа среща. Ако служител поиска физическа среща, срещата ще се проведе в разумен срок в съответствие с местното законодателство.
  - **Алтернатива 3:** Анонимни или поверителни съобщения чрез канала за докладване на сигнализиращи лица на Групата до екипа за подаване на нередности: <https://report.whistleb.com/embracer>.
  - **Алтернатива 4:** Докладване по външни канали, поддържани от компетентните органи или, където е приложимо, институциите, органите или агенциите на ЕС чрез техните външни канали за докладване. Външно докладване до определен орган може да се извършва при условие, че нарушението попада в юрисдикцията на компетентния орган. Когато се докладва външно, съответният орган е този, който отговаря за

получаването на сигнала, предоставянето на необходимата информация и последващите действия. Допълнителна информация относно външното докладване е посочена в специфичните за държавите приложения към настоящите насоки.

- 4.2 Предлагаме избор за докладване към канала на групата, управляван от Embracer Group HQ (Алтернатива 3), или да докладвате на ниво местна оперативна група/дъщерно дружество, като използвате каналите, достъпни на адрес: <https://report.whistleb.com/embracer>. Докладите чрез дъщерни канали се управляват от представители на това юридическо лице.
- 4.3 Всички получени съобщения ще бъдат обработени поверително. За тези, които желаят да останат анонимни, предлагаме канали за анонимно докладване. Каналите за сигнализиране за нередности, позволяващи анонимни съобщения, се администрират от WhistleB, външен доставчик на услуги. Всички съобщения са криптирани. За да гарантира анонимността на лицето, което изпраща съобщение, WhistleB изтрива всички мета данни, включително IP адреси. Лицето, което изпраща съобщението, също остава анонимно в последващия диалог с отговорните получатели на доклада. Докладите могат да бъдат подадени чрез специалната уеб страница на адрес: <https://report.whistleb.com/embracer> от всяко устройство и на всеки език или по телефона (услуга по избор), като в този случай докладващият може да се обади и да остави защитено записано гласово съобщение чрез нашата услуга за телефонен секретар, предоставена от WhistleB. Местни телефонни номера и допълнителни инструкции можете да намерите на адрес: <https://report.whistleb.com/en/message/embracer/phone>.
- 4.4 Моля, имайте предвид, че в определени държави може да съществуват специфични изисквания и ограничения за използването на услуга за подаване на сигнали за нередности. Моля, вижте повече информация на адрес: <https://report.whistleb.com/embracer> — където ще бъдат показани специфични ограничения при избора на вашия език и в специфичните за държавата приложения към тези насоки, Приложения А-О.

## **5. Процесът на разследване**

### **5.1 Екипът за подаване на сигнали**

- 5.1.1 Достъпът до съобщенията, получени чрез нашите канали за подаване на сигнали за нередности, е ограничен до определени лица в Embracer Group AB (дружеството майка) или на всяка местна оперативна група/спомогателно ниво с правомощията да разглеждат случаи на сигнализиране за нередности. Действията им се регистрират и обработката е поверителна. При необходимост лица, които могат да добавят експертни познания, могат да бъдат включени в процеса на разследване, след съгласието на подаващия сигнал, в случай че се разкрие самоличността на докладващото лице. Тези лица имат достъп до съответните данни и също така са обвързани с поверителност.

5.1.2 Ако дадено лице съобщи за притеснение директно на ръководител „Човешки ресурси“, мениджър, местен служител за съответствие или функция или като се свърже лично с екипа за подаване на сигнали за нередности, съобщението се разглежда съгласно настоящите Насоки.

## 5.2 Получаване на съобщение

5.2.1 След получаване на съобщение, екипът за подаване на сигнали решава дали да приеме или отхвърли съобщението. Ако съобщението бъде прието, ще бъдат предприети подходящи мерки за разследване, моля, вижте раздела 5.3 Разследване по-долу.

5.2.2 Подаващият сигнал ще получи потвърждение за получаване на доклада в срок от седем (7) дни.

5.2.3 Екипът за подаване на сигнали за нередности не може да разследва съобщеното неправомерно поведение, ако:

- предполагаемото поведение не подлежи на докладване съгласно настоящите Насоки за подаване на сигнали за нередности
- съобщението не е направено добросъвестно или е злонамерено
- няма достатъчно информация, която да позволи по-нататъшно разследване
- темата на съобщението вече е разрешена

5.2.4 Ако съобщението включва въпроси, които не фигурират в обхвата на настоящите насоки за сигнализиране за нередности, екипът за подаване на сигнали за нередности следва да предостави на докладващото лице подходящи инструкции.

5.2.5 Екипът за сигнализиране за нередности ще изпрати подходяща обратна връзка в рамките на три (3) месеца от датата на получаване на доклада.

5.2.6 Не включвайте чувствителна лична информация за никого, посочен във вашето съобщение, освен ако не е необходимо за описание на вашата загриженост.

## 5.3 Разследване

5.3.1 Всички съобщения се третират сериозно и в съответствие с настоящите насоки за подаване на сигнали за нередности.

- Никой от екипа за подаване на сигнали за нередности или някой, участващ в процеса на разследване, няма да се опита да идентифицира подаващия сигнала.
- Екипът за подаване на сигнали за нередности може, когато е необходимо, да изпрати допълнителни въпроси чрез канала за анонимна комуникация.
- Съобщение няма да бъде разследвано от някой, който може да е замесен или свързан с нарушението.
- Екипът за подаване на сигнали за нередности решава дали и как трябва да се ескалира съобщението за подаване на нередности.

- Съобщенията за подаване на сигнали за нередности се обработват поверително от участващите страни.

## **6. Защита и поверителност**

### **6.1 Защита на лицата, подаващи сигнали**

- 6.1.1 Лице, което изразява искрено подозрение или опасения съгласно настоящите Насоки, няма да бъде изложено на риск да загуби работата си или да понесе някаква форма на санкции или лични неблагоприятни последици в резултат на това. Няма значение дали подателят на сигнал греша, при условие че той или тя действа добросъвестно.
- 6.1.2 Поради съображения относно неприкосновеността на личния живот на лицата, срещу които са били повдигнати обвинения, и всякакви други въпроси, свързани с поверителността, подателят на сигнала ще бъде информиран за резултатите от разследването на обвиненията.
- 6.1.3 В случаите на предполагаеми престъпления неанонимният подател на сигнали ще бъде информиран, че може да се наложи неговата/нейната самоличност да бъде разкрита по време на съдебното производство.

### **6.2 Архивиране на отчет и обработка на лични данни**

- 6.2.1 Независимо дали вашият доклад се получава директно от функцията за сигнализиране за нередности или чрез друг канал, събраната информация се прехвърля на функцията за сигнализиране за нередности за проследяване и архивиране. Това е за да се осигури максимална защита на Вашите данни и да се гарантира, че данните Ви са изчистени правилно.
- 6.2.2 Личните данни, включени в докладваното дело, се обработват с правното основание на законово задължение за получаване, разследване и действие по Вашия доклад и предприемане на всякакви свързани с това мерки. Личните данни се обработват, докато делото е в ход и за период от дванадесет (12) месеца след архивирането на случая, освен ако приложимото законодателство не предвижда различен срок на съхранение. Това е, за да може да се проследяват случаите след приключването им и да могат да се възобновят дела, ако това се изисква поради законодателството или обстоятелствата по делото.
- 6.2.3 Когато Вашите лични данни се обработват поради законово задължение, имате право да коригирате личните си данни и достъпа до тях.
- 6.2.4 Ако имате въпроси относно обработването на лични данни или ако искате да упражните някое от правата си, можете да се свържете с длъжностното лице по защита на данните на Embracer Group AB на адрес: [dro@embracer.com](mailto:dro@embracer.com). Също така имате право да подадете жалба относно обработването на личните си данни до Вашия местен надзорен орган, който в Швеция е IMY, шведският надзорен орган за личните данни. [www.imy.se](http://www.imy.se).





## **7. Приложения**

Допълнения А-О — Допълнения, специфични за държавата

## Приложение С - Специфични разпоредби за страната - България

### Докладване на опасения

Настоящите насоки се прилагат за докладване на такива нарушения, които застрашават или увреждат **обществения интерес** и правото на Европейския съюз и които попадат в съществения обхват на българския Закон за защита на лицата, подаващи сигнали за нередности (*Закон за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения*) (наричан по-нататък "**Закон**"), които са следните:

1. Неправомерни действия в нарушение на правото на Европейския съюз и на България, попадащи в обхвата на Директивата за подаване на сигнали за нарушения, както е посочено в раздел 3.1 в Насоките за подаване на сигнали за нарушения ("**Обхватът**") по-горе;
2. Извършено престъпление от общ характер, за което подателят на сигнала е узнал във връзка с изпълнението на служебните си задължения;
3. Неправомерни действия в нарушение на българското законодателство, които се отнасят до следните области:
  - правилата за изплащане на просрочени публични държавни и общински вземания;
  - правилата на трудовото право;
  - законодателството, свързано с изпълнението на обществените услуги.

Следните видове нарушения не попадат в съществения обхват на Закона:

1. Нарушения на правилата за възлагане на обществени поръчки, включващи аспектите на отбраната или националната сигурност, обхванати от член 346 от ДФЕС;
2. Нарушения на защитата на класифицирана информация по смисъла на българския Закон за защита на класифицираната информация;
3. Нарушения, които са станали известни на лица, упражняващи юридическа професия и за които съществува законово задължение да спазват професионалната тайна;
4. Нарушения на поверителността на здравната информация, както е определено в българския Закон за здравето;
5. Нарушаване на тайната на съдебно заседание;
6. Нарушения на правилата на наказателното производство.

### Кой може да подаде сигнал?

Доклади, които попадат в съществения обхват на Закона, могат да бъдат подавани от следните лица, които са узнали за нарушението по време на или във връзка с изпълнението на своите трудови или служебни задължения или във всякакъв друг **контекст, свързан с работата**:

1. работник, държавен служител или друго лице по трудово правоотношение, независимо от естеството на работата, начина на заплащане и източника на финансиране;
2. лице, което работи без трудов договор и/ или е на свободна практика и/или е занаятчия;
3. доброволец или стажант;
4. съдружник, акционер, едноличен собственик на капитала, член на управителен или надзорен орган на търговско дружество, член на одитния комитет на предприятие;
5. лице, което работи за физическо или юридическо лице, за неговите подизпълнители или доставчици;
6. кандидат за работа, който е получил информация за нарушение в това си качество;
7. работник, който е получил информацията в рамките на трудово или служебно правоотношение, което е било прекратено към момента на докладването;
8. всеки друг подател на сигнал, който докладва за нарушение, за което е разбрал във връзка с работата си.

## Как да подадем сигнал?

За доклади, които не попадат в съществения обхват на Закона или не се отнасят до българско предприятие, можете да подадете сигнал, както е посочено в раздел 4.1 в Насоките за подаване на сигнали за нарушения.

За докладите, които попадат в съществения обхват на Закона, има различни начини за изразяване на загриженост:

1. **Алтернатива 1:** Свържете се със служителя, отговарящ за получаването, регистрирането и разследването на сигнали, подадени в съответния български филиал на Embracer.

### **За Дека Геймс ЕООД съответните данни за контакт са следните:**

- Име: Борислав Милков
  - Телефон: +35 988 619 28 27
  - Емейл: bobby@decagames.com
  - Адрес: ул. „Ангел Каралийчев“ 16А ., Велико Търново 5000, България
  - Лична среща в рамките на подходящ срок, договорен между вас и отговорния служител.
2. **Алтернатива 2:** Конфиденциални съобщения чрез канала за подаване на сигнали за нарушения на Групата до служителя, който отговаря за получаването, регистрирането и разследването на докладите, подадени до Вашия работодател: <https://report.whistleb.com/embracer>.

3. **Алтернатива 3:** Докладване към външния канал, управляван от българската Комисия за защита на личните данни. Докладите до Комисията могат да се подават по един от следните начини:
- В **писмен вид:** по имейл на адрес: [whistleblowing@cpdp.bg](mailto:whistleblowing@cpdp.bg); по пощата на адрес: гр. София 1592, бул. "Проф. Цветан Лазаров" 2
  - **Устно:** на място в Комисията за защита на личните данни на адрес: гр. София 1592, бул. "Проф. Цветан Лазаров" 2

Допълнителна информация за външното докладване може да бъде намерена на уебсайта на Българската комисия за защита на личните данни на адрес: [https://www.cdpd.bg/?p=sub\\_rubric&aid=285](https://www.cdpd.bg/?p=sub_rubric&aid=285).

Анонимното докладване не е разрешено за България. Няма да се образува производство по анонимни сигнали, които попадат в съществения обхват на закона.

Докладите трябва да съдържат поне следната информация:

1. трите имена на подателя, адрес и телефонен номер, както и имейл адрес, ако има такъв;
2. имената на лицето, срещу което е подаден сигналът, както и неговото работно място, ако сигналът е подаден срещу конкретни лица и те са известни;
3. конкретни данни за действителното или потенциалното нарушение, мястото и времето на нарушението, ако то вече е извършено, описание на действието или ситуацията, както и други обстоятелства, доколкото те са известни на подателя на сигнала;
4. дата на подаване на доклада;
5. подпис, електронен подпис или друга идентификация на изпращача.

За да се гарантира, че са спазени всички специфични местни изисквания по отношение на съдържанието и формата на доклада, препоръчваме да се използва образецът на доклада, одобрен от Комисията за защита на личните данни. Образецът може да бъде намерен на уебсайта на Комисията на следния адрес:

[https://www.cdpd.bg/?p=sub\\_rubric&aid=282](https://www.cdpd.bg/?p=sub_rubric&aid=282) (на български език)

[https://www.cdpd.bg/en/index.php?p=sub\\_rubric&aid=282](https://www.cdpd.bg/en/index.php?p=sub_rubric&aid=282) (на английски език)

## Архивиране на доклади

Докладите, които попадат в съществения обхват на закона, както и всички приложени към тях документи, включително последващата документация, свързана с разследването им, се съхраняват за срок от 5 години след приключване на съответното дело, освен в случаите, когато във връзка с подадения доклад се води наказателно, гражданско, трудово и/или административно производство, където 5-годишният срок на съхранение започва да тече след приключване на официалното производство.