

 Open the whistle



ПРАКТИЧЕСКО РЪКОВОДСТВО ЗА ПОДАВАНЕ НА СИГНАЛИ



Съфинансирано от
Европейския съюз

Проектът „Open the Whistle: Защита на лицата, подаващи сигнали, чрез прозрачност, сътрудничество и стратегии за отворено управление“ (OPWHI) е съфинансиран от Европейския съюз (Проект: 101140801 — Покана: CERV-2023-CHAR-LITI-WHISTLE) и има за цел да създаде подкрепяща среда за безопасно подаване на сигнали за нарушения на правото на Съюза и други нарушения, както и да насърчи изграждането на култура, при която лицата, подаващи сигнали, могат да говорят открито без да се притесняват от негативни последици.

2025 Transparency International España

ISBN: 978-84-09-73335-4



Текстът е лицензиран под [Криейтив Комънс Признание-Некомерсиално-Без производни 4.0 Международен Лиценз](https://creativecommons.org/licenses/by-nc-nd/4.0/).

Графична концепция и заглавни страници: Алесиа Риоло

Дизайн и предпечатна подготовка: Алваро Арибас Хименес



Съфинансирано от
Европейския съюз

Съ-финансирано от Европейския съюз. Изразените възгледи и мнения обаче принадлежат изцяло на техния(ите) автор(и) и не отразяват непременно възгледите и мненията на Европейския съюз или на Европейската изпълнителна агенция за образование и култура (EACEA). За тях не носи отговорност нито Европейският съюз, нито EACEA.

ПАРТНЬОРИ ПО ПРОЕКТА

Libera – Associations names and numbers against mafias (Libera)¹ е мрежа от организации на гражданското общество, ангажирани в противодействието на корупцията и организираната престъпност, както и на техните поддръжници, с цел насърчаване на социалната справедливост и демокрацията. Основана в Италия през 1995 г., мрежата в момента включва 278 местни групи и 80 международни организации от 35 страни в Европа, Западните Балкани, Африка и Латинска Америка. От 2016 г. насам тя участва активно в защитата на лицата, подаващи сигнали за нередности, по-специално чрез Linea Libera, служба за изслушване и предоставяне на подкрепа на лица, сигнализиращи за нередности в публичния и частния сектор. Libera си сътрудничи тясно с Националния орган за борба с корупцията (ANAC) в Италия, публичните администрации, други граждански организации и местните общности за по-добра защита на лицата, сигнализиращи за нередности, и за насърчаване на съвместни инициативи срещу корупцията.

University of Pisa (UNIPi).² От 2010 г. Факултетът по политически науки на Университета в Пиза организира магистърска програма по „Анализ, превенция и борба с организираната престъпност и корупцията“, в рамките на която повече от двеста студенти от цяла Италия и чужбина са обучени за борба с корупцията и мафията. UNIPi ръководи и Обсерваторията за политическа корупция.

Transparency International Spain (TI-E).³ Чрез мониторинг на обществените политики, застъпничество, кампании и изследвания, TI-E работи за по-голяма прозрачност и почтеност във всички области на обществения живот. TI-E се стреми да насърчава и укрепва култура на прозрачност, почтеност, откритост и отчетност в испанския публичен сектор чрез диалог, колективни действия, обучение и съвместна работа с публичните администрации и правителството. Организацията участва активно в проектирането, разработването, мониторинга и оценката на публичните политики за предотвратяване на корупцията и за „отворено управление“, насърчава прилагането на принципите и ангажиментите на „отвореното управление“ в Испания и е част от няколко групи за подаване на сигнали за нередности. Във всички свои действия тя интегрира принципа на равенството между половете, като идентифицира междусекторните неравенства и признава диференцираното въздействие на корупцията и липсата на прозрачност.

Center for the Study of Democracy (CSD).⁴ Основан в края на 1989 г., CSD е интердисциплинарен научноизследователски институт с регионална насоченост към Европа и Западните Балкани. Публикувал е редица доклади, наръчници и ръководства за защита на правата на човека, върховенство на правото и борбата с корупцията. Като утвърден

¹ Libera - Associazioni, nomi e numeri contro le mafie.

² Università di Pisa.

³ Transparencia Internacional España.

⁴ Център за изследване на демокрацията.

антикорупционен фактор в региона и член на Коалицията за защита на лицата, сигнализиращи за нередности (SECWP) организацията участва активно в подобряването на политиките и културата за подаване на сигнали. CSD работи активно за транспонирането в България на Директива 2019/1937/ЕС относно защитата на лицата, подаващи сигнали за нередности. Негови експерти участваха в работната група на Министерството на правосъдието на Република България, която изготви законопроекта за транспониране на Директива 2019/1937/ЕС, и представиха становища и коментари по законопроектите, внесени в парламента.

National Anti-Corruption Authority (ANAC).⁵ ANAC е органът, който отговаря за получаването и разследването на сигнали за нарушения, както и за ответни действия, предприети срещу лица, подаващи сигнали за нередности. ANAC защитава тайната на самоличността на подателя на сигнала и съдържанието на сигналите и може да комуникира анонимно с лицето, сигнализиращо за нередности като използва система за криптиране на ИТ платформата. Правомощията на ANAC за налагане на санкции обхващат предприемането на ответни действия, случаи на бездействие от страна на отговорни служители, които не са проверили и анализирали получения сигнал, и случаи на липса на система за управление на сигналите.

Anti-Fraud Office of Catalonia (OAC).⁶ ОАС е публична институция, създадена със закон № 14/2008 на 5 ноември 2008 г. с цел да се предотвратява и разследва случаи на незаконно използване или разпределяне на публични средства или друго неправомерно присвояване вследствие на действия, свързани с конфликт на интереси или използване за лична изгода на информация, произтичаща от присъщите функции на държавните служители. Институцията предоставя и съвети и препоръки за приемане на мерки срещу корупцията, измамите и друго поведение, което е в нарушение на почтеността и прозрачността. На Службата са поверени и функциите, които Закон № 2/2023 за транспониране на Директива 1937/2019/ЕС възлага на Независимия орган за защита на сигнализиращите лица към ОАС. Тя може да налага и санкции за нарушения на Закон № 2/2023 от 20 февруари 2023 г., уреждащ защитата на лицата, които съобщават за нарушения на нормативната уредба, и борбата с корупцията.

Commission for Personal Data Protection (CPDP).⁷ Комисията за защита на личните данни в България е централен национален орган за външно подаване на сигнали за нередности. CPDP предоставя защита на физическите лица, като взема предвид условията, реда и мерките за защита на лицата, сигнализиращи за нередности в публичния и частния сектор, които подават сигнали, или публично оповестяват информация за нарушения на българското законодателство или актове на Европейския съюз, които застрашават или увреждат обществения интерес и правото на Европейския съюз. Комисията разяснява реда и условията за подаването и разглеждането на такива сигнали или публично оповестяване на информация.

⁵ *Autorità Nazionale Anticorruzione.*

⁶ *Oficina Antifrau de Catalunya.*

⁷ *Комисия за защита на личните данни.*

БЛАГОДАРНОСТИ

Партньорите изразяват благодарността си за безценния принос на всички експерти, представители на партньорите по проекта и всички, които участваха в разработването на това ръководство.

Работна група

ANAC	Джулия Косу Джовани Паоло Селито Валентина Томаси
CSD	Димитър Марков Мария Йорданова
CPDP	Десислава Тошкова-Николова Атанаска Георгиева Кристина Радкова-Станева Катя Станимирова Христо Аламинов Йоан Ангелов Радостина Такова
Libera	Леонардо Феранте Елиза Орландо Карлота Бартолучи
ОАС	Елисенда Ескода Мариса Мирайес Оскар Рока Жорди Трес
TI-E	Давид Мартинес Гарсия Айлин Рубио Ариета Камила Чела Андреа Ривера
UNIFI	Алберто Ванучи Франческа Рисполи Мартина Каталдо Еуженио Пицименти

Научен комитет на проекта

Лаура Вали, ANAC
Масимилиано Андрета, UNIFI
Роберта Брачиале, UNIFI
Валентина Мария Донини,
National School of Administration
(SNA)⁸
Венцислав Караджов, CPDP
Деляна Досева, CSD
Елизабет Мартинес, ОАС
Силвина Бачигалупо Сагезе, TI-E
Рамон Рагес и Валес, UPF

⁸ Scuola Nazionale dell'Amministrazione.

СЪДЪРЖАНИЕ

ВЪВЕДЕНИЕ И СТРУКТУРА НА РЪКОВОДСТВОТО	СТР. 6
ГЛАВА 1: ПРОЗРАЧНОСТ И КОМУНИКАЦИЯ НА СИСТЕМИТЕ ЗА СИГНАЛИЗИРАНЕ	СТР. 13
ГЛАВА 2: ПРАВИЛНО РАЗСЛЕДВАНЕ И УПРАВЛЕНИЕ В РАМКИТЕ НА ВЪТРЕШНИТЕ СИСТЕМИ ЗА ПОДАВАНЕ НА СИГНАЛИ ЗА НЕРЕДНОСТИ	СТР. 35
ГЛАВА 3: ЗАЩИТА НА ЛИЧНИТЕ ДАННИ	СТР. 62
ГЛАВА 4: ЗАЩИТА И ПОДКРЕПА НА ЛИЦАТА, ПОДАВАЩИ СИГНАЛИ ЗА НЕРЕДНОСТИ	СТР. 86
ГЛАВА 5: ИЗМЕРВАНЕ И ОЦЕНКА НА ЕФЕКТИВНОСТТА НА СИСТЕМАТА И ОЦЕНКА НА КУЛТУРАТА НА ПОДАВАНЕ НА СИГНАЛИ ЗА НЕРЕДНОСТИ	СТР. 104
ГЛАВА 6: ПРЕПОРЪКИ ОТНОСНО РАВЕНСТВОТО МЕЖДУ ПОЛОВЕТЕ И ОТКРИТОТО УПРАВЛЕНИЕ	СТР. 120
ОТВЪД РЪКОВОДСТВОТО	СТР. 124

ВЪВЕДЕНИЕ И СТРУКТУРА НА РЪКОВОДСТВОТО

КАКВА Е ЦЕЛТА НА ТОВА РЪКОВОДСТВО?

Това ръководство е резултат от **знанията**, научните изследвания и упоритата работа на институциите, академичните среди и организациите на гражданското общество от **Италия**, **България** и **Испания**. То съдържа набор от инструменти и има за цел да предостави теоретични знания и практически насоки за създаване на нова представа и стабилен модел за защита на лицата, сигнализиращи за нередности. Необходимо е да се **гарантира безопасна и подкрепяща среда** за сигнализиращите лица и да се **улесни ефективното докладване на неправомерно поведение**.

Ръководството изследва **пет основни аспекта на подаването на сигнали** за нередности, структурирани в пет глави, предлагащи нови идеи и практически препоръки за прилагане на **добри практики и насърчаване на нови виждания** за подаване на сигнали:

- Глава 1 → Прозрачност и комуникация на системите за сигнализиране
- Глава 2 → Правилно разследване и управление в рамките на вътрешните системи за подаване на сигнали за нередности
- Глава 3 → Защита на личните данни
- Глава 4 → Защита и подкрепа на лицата, подаващи сигнали за нередности
- Глава 5 → Измерване и оценка на ефективността на системата и оценка на културата на подаване на сигнали за нередности

Като снабдява **различните заинтересовани страни** с подходящи инструменти и знания, това ръководство:

- предоставя информация за **стандартизирани механизми за докладване, мерки за поверителност и политики срещу ответни действия**.
- разглежда предизвикателствата в националното законодателство за подаване на сигнали за нередности и проблемите, произтичащи от **транспонирането на Европейската директива 2019/1937/ЕС (наричана по-долу „Директивата“)**, като се стреми да преодолее съществуващите пропуски или, когато това не е възможно, да посочи нерешените въпроси.
- прави **динамичен анализ**, като разглежда развитието на отговорите на Директивата и идентифицира **текущите предизвикателства след шест годишно прилагане**.
- дава **конкретни предложения въз основа на поуките, извлечени през този период**, които могат да бъдат използвани при бъдещи подобрения.

Освен това ръководството препоръчва **добри практики за насърчаване на култура на прозрачност**, отчетност и етична отговорност, като в крайна сметка укрепва институциите и повишава общественото доверие.

ТОВА РЪКОВОДСТВО НЕ Е:

- **наръчник**: то не предоставя **задълбочен анализ на Директивата** или изчерпателни **специфични за всяка държава оценки**. То не служи и като категорична отправна точка за оценка на съответствието.
- **документ** от само една гледна точка: то не разглежда подаването на сигнали само от правна, политическа или икономическа гледна точка. Вместо това **интегрира множество дисциплини и подходи**, за да осигури цялостно разбиране, признавайки многостранния **характер на подаването на сигнали**.
- **исторически или теоретичен анализ**: то избягва да се задълбочава в **историята или теоретичните основи на подаването на сигнали**, като вместо това се фокусира върху **практически проблеми** и препоръки, които могат да бъдат използвани.
- **едностранчив документ**: то не се съсредоточава нито само върху функционирането на системата, нито само върху защитата на лицата, сигнализиращи за нередности, а вместо това признава **значението на двете гледни точки** и се стреми да ги хармонизира.

ФОКУС ВЪРХУ ДВА ХОРИЗОНТАЛНИ ПОДХОДА: ОТВОРЕНО УПРАВЛЕНИЕ И РАВЕНСТВО МЕЖДУ ПОЛОВЕТЕ

Във всяка от отделните глави ръководството обединява два основни подхода: **подхода, основан на равенството между половете, и подхода, основан на отвореното управление**.

- **Подходът, основан на равенството между половете**, има за цел да **повиши осведомеността** относно значението на разработването на достъпни, приобщаващи и **чувствителни към аспектите на пола системи за подаване на сигнали** за нередности с цел ефективно и всеобхватно докладване и защита. През последните години все по-често се признава, че различията между половете могат да повлияят непропорционално на жените, мъжете и лицата с друга пола идентичност, като се подчертава необходимостта от чувствителни към пола механизми за подаване на сигнали за нередности. Това помага да се **преодолеят недостатъците в механизмите за правна защита и политиките**, които обикновено не отчитат различията между половете и често пренебрегват съображенията за многообразие, равенство и недискриминация. В този контекст идеята е да се **предоставят както теоретични, така и практически инструменти** на всички заинтересовани страни, участващи в подаването на сигнали за нередности, като се улесни ефективното интегриране на подхода, основан на равенството между половете.
- **Подходът на отвореното управление** има за цел да формулира препоръки за **справяне с предизвикателствата, свързани с подаване на сигнали за нередности**, на базата на основните

принципи на отвореното управление, като **прозрачност, отчетност, участие и приобщаване**. С други думи, всички действия, които гражданското общество и институциите могат да предприемат колективно и съвместно, за да насърчат подаването на сигнали за нередности и да защитят сигнализиращите лица. Ако вашата страна е член на Партньорството за отворено управление (OGP), авторите предлагат всеки такъв ангажимент да бъде част от циклите на Националния план за действие⁹ или част от предизвикателството Open Gov¹⁰, което позволява да бъдат поети и признати амбициозни ангажименти за реформи извън редовния цикъл на плана за действие. По този начин ще бъде по-лесно да се **установят прозрачни отношения с всички заинтересовани страни, да се създават съвместни решения и да се наблюдава по-добре тяхното изпълнение и въздействие**.

Защо подаването на сигнали за нередности има значение? Необходимост от превръщането му в съществен и системен компонент на обществото

Подаването на сигнали е термин, който носи множество значения и нюанси. В широк смисъл това е **„форма на докладване“**, която играе решаваща роля за гарантирането на отчетност, разкриването на злоупотреби и корупция, изобличаване на скрити нарушения и предотвратяване на вреди. Лицата, подаващи сигнали за нередности, често стават свидетели на нарушения и действат в обществен интерес, за да предотвратят настъпването на вреди. Те имат право на справедливо отношение, уважение и **защита** от ответни действия. Въпреки това, за да бъде подаването на сигнали за нередности наистина ефективно, то **трябва да бъде интегрирано** като **основен и системен компонент** на работното място и в обществото.

Силната правна защита, ясните механизми за докладване и културата, която насърчава **етичната отговорност**, са от решаващо значение за овластяването на хората да говорят без страх от отмъщение. Понастоящем нормите на поведение в организациите и обществото могат да обезкуражат хората да говорят за престъпления или етични нарушения: необходима е промяна на все още разпространената концепция за сигнализиращото лице като **доносник или предател** и на идеята, че подаването на сигнали за нередности е **„extrema ratio“** и изисква огромни правни усилия. Тези разбирания са проблематични, защото вместо да се разглежда като структурен елемент на която и да е организация, подаването на сигнали все още се възприема като извънредна **мярка, която изисква изключителна намеса**. С институционализирането на подаването на сигнали като основна практика се създава по-безопасна, прозрачна и отговорна среда за всички.

⁹ Виж също: <https://www.opengovpartnership.org/process/action-plan-cycle/>

¹⁰ Виж също: <https://www.opengovpartnership.org/the-open-gov-challenge/open-government-challenge-areas/>

ДВЕ РАЗЛИЧНИ, НО ДОПЪЛВАЩИ СЕ ГЛЕДНИ ТОЧКИ

Този документ се стреми да балансира **две гледни точки**:

- подходът, **ориентиран към „подаването на сигнали“**, прилаган от компетентните органи, отговарящи за функционирането на системата.
- подходът, **ориентиран към „лицата, сигнализиращи за нередности“**, възприет от организациите на гражданското общество, които са загрижени за лицето, което сигнализира, възнамерява да сигнализира или изпитва последиците от подадения сигнала, и се стремят да гарантират, че неговите житейски планове няма да пострадат.

КРАТКА ИСТОРИЯ НА ЕВРОПЕЙСКАТА ДИРЕКТИВА 2019/1937/ЕС И НЕЙНОТО ТРАНСПОНИРАНЕ

През 2016 г. Европейската комисия приема, че **няма правно основание** за приемане на директива за подаване на сигнали за нередности, но е необходимо хармонизиране на законодателството на ЕС относно защитата на сигнализиращите лица. Едва през 2019 г., в отговор на поредица от **нашумели скандали** (напр. LuxLeaks и „Досиетата от Панама“), Европейският парламент и Съветът приемат Директивата на ЕС относно подаването на сигнали за нередности. Целта е да се установи минимален **стандарт за защита на лицата, сигнализиращи за нередности, във всички държави – членки на ЕС**, като се гарантира, че лицата, които съобщават за нарушения на правото на ЕС, са защитени от **ответни действия с цел отмъщение**. На държавите – членки на ЕС, е даден срок до **17 декември 2021 г.** да транспонират Директивата в националното си законодателство. От 2024 г. повечето държави членки са включили **Директивата в своите правни системи**, въпреки че някои държави са **изправени пред предизвикателства** при осигуряването на пълно съответствие. Националното законодателство в отделните държави се различава значително по отношение на условията, при които на лицата, сигнализиращи за нередности, се предоставя защита, както и на правното основание за това.

ПОДАВАНЕ НА СИГНАЛИ В ИТАЛИЯ

В **Италия** подаването на сигнали за нередности е регулирано и преди Директивата на ЕС, като първите мерки са въведени през 2012 г. и са разширени по-късно през 2017 г. Закон № 190/2012 е първият закон в **Италия**, който въвежда специална защита за лицата, сигнализиращи за нередности, въпреки че е ограничен до публичния сектор. Този закон позволява на държавните служители да съобщават за неправомерно поведение, за което са разбрали на работното си място, без да търпят ответни действия. Защитата обаче е слаба: разпоредбите само забраняват дисциплинарните санкции срещу лицата, сигнализиращи за нередности, но не предвиждат реална система за защита или ясни

механизми за гарантиране на поверителността на сигналите. Освен това няма гаранции за служителите в частния сектор. Закон № 179/2017 укрепва рамката, като въвежда по-широка защита както в публичния, така и в частния сектор. Той установява мерки за гарантиране на конфиденциалността на лицата, подаващи сигнали за нередности, и налага санкции на тези, които се опитват да им отмъстят. Освен това той изисква от частните дружества, отговарящи на определени критерии, да създадат и поддържат вътрешни канали за подаване на сигнали.

И накрая, в съответствие с Директивата, новият закон за подаване на сигнали за нередности (Законодателен указ № 24/2023) изисква от публичните и частните субекти с повече от 50 служители да създадат вътрешни канали за подаване на сигнали, които гарантират поверителност. Могат да се подават сигнали и до ANAC (външния канал), ако вътрешните канали са ненадеждни, неефективни или ако нарушението представлява непосредствен обществен риск. Със закона се въвежда признаване на организациите от третия сектор, които подкрепят лицата, сигнализиращи за нередности, преди и след подаването на сигнали. Законът има за цел да подобри гаранциите срещу ответни мерки и да засили механизмите за сигнализиране, като разшири тази защита и освен служителите да бъдат обхванати и лица със свободни професии, доброволци, стажанти, акционери и лица, осигуряващи групови комуникации.

ПОДАВАНЕ НА СИГНАЛИ В БЪЛГАРИЯ

Преди транспонирането на Директивата в **България** има разпоредби, свързани със защитата на лицата, сигнализиращи за нередности, разпръснати в различни закони. Законът за защита от дискриминация забранява отмъщението срещу лица, които подават жалби за дискриминация, докато Административнопроцесуалният кодекс предлага общи гаранции за тези, които съобщават за злоупотреба с власт или корупция. В обработката на такива сигнали участват няколко органа, включително Главният инспекторат на Министерския съвет, инспекторатите на министерствата и Комисията за борба с корупцията, която служи като централен орган за получаване на сигнали за корупция и конфликт на интереси. Освен това някои публични институции и частни дружества, особено тези, които извършват дейност в международен план или в регулирани сектори, разработват и прилагат механизми за вътрешно сигнализиране.

Тази, макар и фрагментирана, рамка помага за улесняване на транспонирането на Директивата в националното законодателство. През 2023 г. **България** приема Закона за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения, който е в сила от 2 февруари 2023 г. Законът задължава работодателите от публичния и частния сектор с 50 или повече работници и служители да създадат вътрешни канали за подаване на сигнали, като задължението за частните работодатели с между 50 и 249 служители е в сила от 17

декември 2023 г. Комисията за защита на личните данни (CPDP) е определена за централен орган за външно подаване на сигнали и своевременно предприема важни стъпки за прилагане на законодателството.

ПОДАВАНЕ НА СИГНАЛИ В ИСПАНИЯ

Съгласно Наказателно-процесуалния закон (*Ley de Enjuiciamiento Criminal* или LECrim), действащ от 1882 г., лицата в **Испания**, които са свидетели на престъпления, имат законово задължение да докладват за тях, под заплахата от санкции при неспазване. Това задължение се разпростира върху „ключовите свидетели“ (член 264 от LECrim) и някои професии, например в публичните органи, които са заплашени от по-строги наказания при несъобщаване за престъпление (член 262 от LECrim и член 408 от испанския Наказателен кодекс).

От друга страна, реформата на испанския Наказателен кодекс от 2015 г. въвежда изискването програмите за съответствие да включват задължение за докладване на „възможни рискове и нарушения на органа, отговорен за надзора върху функционирането и прилагането на модела за превенция“ (член 31а точка 5, параграф 4). Въпреки че Наказателният кодекс не включва това като задължение, при евентуален наказателен процес, лицата, които желаят да получат освобождаване от или смекчаване на отговорността си, трябва да имат вътрешни канали за подаване на сигнали за нередности. На практика това означава, че в **Испания** много частни субекти (особено големите дружества) създават такива механизми преди приемането на Директива 2019/1937/ЕС, разработвайки свои собствени политики и процедури за защита на лицата, сигнализиращи за нередности. В публичния сектор има и някои регулации на регионално равнище, предшестващи Директивата. Така например със Закон № 11/2016 от 28 ноември 2016 г. се създава Агенцията за предотвратяване и борба с измамите и корупцията на автономна област Валенсия. Агенцията е задължена да поддържа поверителни канали, гарантиращи пълна конфиденциалност при изготвянето на сигнала, когато подателят се позовава на процедурата, регламентирана от този закон.

Въпреки това **Испания** не разполага с всеобхватна и последователна защита на лицата, подаващи сигнали за нередности, до транспонирането на Директива 2019/1937/ЕС, осъществено чрез Закон № 2/2023 от 20 февруари 2023 г., уреждащ защитата на лицата, които съобщават за нарушения на нормативната уредба, и борбата с корупцията.



Прозрачност и комуникация на системите за сигнализиране



Глава 1

ПРОЗРАЧНОСТ И КОМУНИКАЦИЯ НА СИСТЕМИТЕ ЗА СИГНАЛИЗИРАНЕ

ГЛАВА 1

1.1. СИСТЕМИТЕ ЗА СИГНАЛИЗИРАНЕ: НЕОБХОДИМОСТ ОТ ЯСНИ НАСОКИ

Доверието¹¹ в системата е ключов фактор за всяко сигнализиращо лице. Липсата на информация за наличните канали и за системата като цяло може да има отрицателно въздействие върху доверието, тъй като доверието не може да бъде изградено единствено върху съществуването на канала. От съществено значение за сигнализирането е наличието на подкрепящата и защитена среда.

Липсата на ясни насоки може да доведе до дезинформация и недоверие, да обезкуражи лицата, подаващи сигнали за нередности, и да възпрепятства създаването на безопасно пространство за подаване на сигнали. Ето защо, за да се **повиши осведомеността и доверието**, е необходимо да се **предостави информация** най-малко за това:

- кой може или трябва да докладва;
- как се докладва;
- кога се докладва;
- на кого се докладва;
- как е защитено сигнализиращото лице;
- какви права има обвиненото лице;
- как работи процесът на подаване на сигнали;
- какви са мерките за сигурност;
- как се гарантира, че системата за подаване на сигнали е чувствителна към равенството между половете.

Според обществена консултация, проведена през 2017 г., **само 15% от гражданите са запознати** със съществуващите правила за защита на лицата, сигнализиращи за нередности, а **49% не знаят къде да докладват за корупция** (ЕС 2018).¹² По подобен начин някои проучвания¹³ показват, че създаването на солидна основа за програма за подаване на сигнали за нередности, т.е. определяне на ясни оперативни процедури или насоки както за държавните служители и останалите служители в държавните органи, така и за лицата, сигнализиращи за нередности, е успешна практика за ефективно

¹¹ Според Binikos (2008) доверието в организацията и управлението оказва положително въздействие върху намеренията да се сигнализира за нарушение според 16 проучвания (между тях: Attree, 2007; Brennan and Kelly, 2007; Binikos, 2008; Curtis and Taylor, 2009; Seifert et al., 2014; и др.).

¹² Виж също: <https://ec.europa.eu/newsroom/just/items/54254/en>

¹³ Australian Securities and Investment Commission, 2023; и др.

разглеждане на сигналите. Тъй като подаването на сигнали за нередности е сложен процес с лични и психологически последици, са необходими организационни и културни мерки в подкрепа на прилагането на закона, като същевременно се вземат предвид културните нагласи към лицата, подаващи сигнали за нередности¹⁴.

Въпреки че Директивата ясно **определя правата и принципите**, тя не съдържа ясни и подробни разпоредби относно прозрачността и информацията, която всички задължени субекти (член 8) трябва да предоставят относно своите **канали и системи**. В член 13 от Директивата се установява общо задължение за компетентните органи, а член 9, параграф 1 предвижда изискване за „предоставяне на ясна и лесно достъпна информация за процедурите за външно подаване на сигнали към компетентните органи съгласно член 10, а когато е уместно – към институциите, органите, службите или агенциите на Съюза“ (член 9, параграф 1, буква ж)).

В резултат на това **лицата, които потенциално биха подали сигнал за нередност**, и други граждани, които се интересуват от подаване на сигнали, може да не бъдат достатъчно информирани за наличните канали, системата за подаване на сигнали, съответните процедури и органи, правата, сроковете, техническата информация, мерките за защита и характеристиките на системата за ИТ сигурност.

В **Испания** раздел IV от Закон № 2/2023 от 20 февруари 2023 г., уреждащ защитата на лицата, които съобщават за нарушения на нормативната уредба, и борбата с корупцията¹⁵ е посветен на регулиране на информацията, която трябва да бъде предоставяна както от задължените субекти, така и от компетентните органи, по отношение на вътрешните и външните канали. Законът изрично предвижда, че тази информация **трябва да бъде видима на уебсайтове** или електронни платформи, в отделни и лесно достъпни секции. Той също така изисква всички субекти, от които се изисква да имат вътрешен канал, както в публичния, така и в частния сектор, да поддържат регистър на получените сигнали и всички вътрешни разследвания, произтичащи от тях. Този регистър, обаче, не е публичен и е достъпен само за съдебните органи.

В член 25 от Закон № 2/2023 изрично се посочва, че **субектите, попадащи в приложното поле на закона**, „предоставят адекватна информация в ясна и лесно достъпна форма за използването на всеки вътрешен информационен канал, който са въвели, както и за основните принципи на процедурата по администриране. Ако имат собствен уебсайт, тази информация се поставя на началната страница, в отделна и лесно разпознаваема секция раздел“.

¹⁴ Teichmann et al., 2022.

¹⁵ Виж също: <https://www.boe.es/buscar/act.php?id=BOE-A-2023-4513>

Законът обаче не определя минималното съдържание, което задължените субектите трябва да включат, когато да информират обществеността през уебсайтовете си за своите системи за докладване¹⁶.

В **Италия** всички публични и частни субекти са длъжни да **предоставят ясна информация за канала**, процедурите и предпоставките за вътрешно подаване на сигнали, както и за канала, процедурите и предпоставките за външно подаване на сигнали¹⁷.

Тази информация **трябва да бъде лесно видима на работното място** и достъпна за лицата, които са в определено правоотношение със задължения субект. Ако задълженият субект има уебсайт, информацията трябва да бъде публикувана в специален раздел. Освен това, в закона¹⁸ се посочва, че като **компетентен орган** за управление на външния канал за подаване на сигнали, ANAC трябва да публикува информация като:

- мерки за защита на лицата, подаващи сигнали за нередности;
- данни за контакт, като например телефонния номер на отдела, който администрира сигналите, като се посочва дали телефонните разговори се записват или не, пощенският адрес и адресът за електронна поща, както обикновения, така и сертифицирания;
- правила за поверителност, приложими за външни и вътрешни сигнали.

В **България** Законът за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения, от 2 февруари 2023 г., в съответствие с Директивата, гласи, че „(...) Задължените субекти са длъжни да предоставят ясна и лесно достъпна информация относно условията и реда за подаване на сигнали. Информацията се предоставя на интернет страниците на задължените субекти, както и на видно място в офисите и работните помещения“ (чл. 12, ал. 4).¹⁹

Въпреки че това задължение е **формално изпълнено, няма оценка на неговата ефективност**.

Съдържателната прозрачност и ефективната комуникация не са незначителни въпроси; те са от съществено значение за правилното

¹⁶ За органите, посочени в член 24, законът е малко по-ясен, като установява, че те публикуват в отделен, лесно разпознаваем и достъпен раздел на своя електронен сайт най-малко следната информация: „(а) условията за допустимост за защитата съгласно този закон; (б) данните за контакт за външните информационни канали, предвидени в раздел III, по-специално електронните и пощенските адреси и телефонните номера, свързани с тези канали, като се посочва дали телефонните разговори се записват; (в) процедурите за администриране, включително начина, по който компетентният орган може да поиска от подателя на сигнала да изясни предоставената информация или да предостави допълнителна информация, срока за отговор, ако има такъв, както и вида и съдържанието на този отговор; (г) режима на поверителност, приложим към сигналите, и по-специално информацията относно обработването на лични данни в съответствие с разпоредбите на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г., Устройствен закон № 3/2018 от 5 декември и раздел VII от настоящия закон; (д) средствата за правна защита и процедурите за защита срещу ответни действия с цел отмъщение, както и възможността за получаване поверителни съвети (включително информацията за предвидените условията за освобождаване от отговорност и смекчаване на санкцията, посочена в член 40); и (е) данните за контакт с независимия орган за защита на лицата, сигнализиращи за нередности, I.W.P.A. или със съответния друг компетентен орган.“

¹⁷ Член 5.1 от Законодателен указ № 24/2023 от 10 март 2023 г.

¹⁸ Член 9 от Законодателен указ № 24/2023 за транспониране на Директива 2019/1937/ЕС.

¹⁹ Закон за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения, 2 февруари 2023 г., чл. 12, ал. 4.

функциониране на системите за подаване на сигнали за нередности. Физическите лица не могат да вземат информирани решения дали, кога и как да докладват, ако не са достатъчно информирани предварително за основните си **права и задължения, основните принципи и стъпките на процеса на докладване**, както и подробности за естеството и функционирането на каналите за подаване на сигнали в рамките на дадена организация или публичен орган²⁰.

Освен това, държавните органи и компетентните надзорни органи могат **по-лесно да упражняват надзор** върху задължените лица, като упражняват контрол за съответствие чрез периодични прегледи на мерките за прозрачност и активно промотиране на достъпни канали за сигнализиране.

Въз основа на прегледа на Директивата, съображения 59 и 75, член 25 от испанския Закон № 2/2023, член 12 от българския закон за защита на сигнализиращите лица, член 5.1 и член 9.1 от **ИТАЛИАНСКИЯ** Законодателен указ № 24/2023 и като се има предвид горепосоченото, може да се заключи, че за да се гарантира адекватна и всеобхватна прозрачност на информационните системи и канали, така че те да могат ефективно да изпълняват своята мисия, трябва да бъдат изпълнени **две основни условия**: едно, свързано със **съдържанието**, и друго, свързано с **формата**.

1.2. ПРОЗРАЧНОСТ ПО ОТНОШЕНИЕ НА ПРАВАТА И ГАРАНЦИИТЕ НА ЛИЦАТА, ПОДАВАЩИ СИГНАЛИ ЗА НЕРЕДНОСТИ, И ЗАСЕГНАТИТЕ/ ОБВИНЕНИТЕ ЛИЦА

Що се отнася до съдържанието, всички задължени субекти трябва да предоставят **ясна, пълна, актуализирана и структурирана информация** най-малко в следните области:

1.2.1. Прозрачност по отношение на правата и гаранциите на лицата, подаващи сигнали за нередности, и засегнатите или обвиняемите лица

Необходимо е да се включи специален раздел (както на уебсайта, така и в интранет, ако е приложимо) с пълен списък на **правата както на лицата, сигнализиращи за нередности**, и на засегнатите лица, така и на трети страни (например лице, което е споменато в сигнала, свидетели, представители на работниците/синдикати, колеги на подателя на сигнала), ако е приложимо.

²⁰ Европейският законодател е много ясен в това отношение: „лицата, които обмислят да подадат сигнал за нарушения на правото на Съюза, следва да могат да вземат информирано решение относно това дали, как и кога да подадат сигнал. От правните субекти в частния и публичния сектор, които разполагат с процедури за вътрешно подаване на сигнали, следва да се изисква да предоставят информация за тези процедури, както и за процедурите за външно подаване на сигнали до съответните компетентни органи. От съществено значение е тази информация да бъде ясна и лесно достъпна, включително, доколкото е възможно, и за лица, освен работници, които са в контакт със субекта чрез свързани с тяхната работа дейности, като например доставчици на услуги, дистрибутори, доставчици и бизнес партньори. Например тази информация може да бъде поставена на видно място, до което имат достъп всички лица, и на уебсайта на субекта, и може да бъде включена в курсове и семинарни обучения по етика и почтеност“ (съображение 59 от Директива 2019/1937/ЕС). Освен това в друго съображение се повтаря, че „цялата информация относно сигналите трябва да бъде прозрачна, лесно разбираема и надеждна, за да се насърчава, а не да се възпрепятства подаването на сигнали“ (съображение 75 от Директива 2019/1937/ЕС).

Що се отнася до лицата, които потенциално биха сигнализирали за нередности, този раздел трябва да включва най-малко:

- защита на поверителността на сигнализиращите лица и на съдържанието на сигналите;
- непредприемане на ответни действия²¹ по смисъла на Директивата и националното законодателство;
- ясна информация за органите, разглеждащи сигнала;
- право на получаване на мотивиран отговор при решение за архивиране, отхвърляне или отказ за разглеждане на сигнала;
- защита на личните данни²²;
- потвърждение за получаване и надлежно проследяване на сигналите;
- своевременно и подходящо уведомление за решението²³;
- справедливо, независимо и безпристрастно разследване;
- правни съвети, правна и психологическа подкрепа или подкрепа от представители на работниците (ако се изисква от закона);
- право на добра администрация по смисъла на член 41 от Хартата на основните права на Европейския съюз (особено за задължените субекти от публичния сектор);
- психологическа подкрепа (ако се изисква от закона или се предлага от субекта);
- финансова подкрепа (ако се изисква от закона или се предлага от субекта).

Що се отнася до обвинените/засегнатите лица, в раздела е необходимо да се включи най-малко информация за:

- презумпцията за невиновност;
- защитата на самоличността/поверителността;
- правото на изслушване;
- правото на достъп до материалите по разследването;
- правото на справедлив процес;
- правото на представяне на доказателства;
- правната защита и представителството на работниците;
- правото на познаване на инструктиращия орган и правото на безпристрастен съдия;
- правата за защита на личните данни.

²¹ Според един от интервюираните експерти е важно да се предоставя информация за това как се предотвратява евентуално отмъщение, как се гарантира защитата на лицата, сигнализиращи за нередности, както и да се очертаят конкретните процеси, осигуряващи тази защита.

²² Включително, но не само: правото на информация за самоличността на администратора на данни, целта на обработването и възможността за упражняване на правата, посочени в членове 15 до 22 от Общия регламент относно защитата на данните (GDPR), както и правото на изтриване на данни след три месеца, освен ако не се касае дисциплинарно, дисциплинарно-наказателно или наказателно производство.

²³ В тази връзка вж. показател № 94 от доклада TRAC-SPAIN за 2022 г. (стр. 159).

На последно място, важно е да се включат и **правата и гаранциите на трети страни**, потенциално свързани, засегнати или посочени в сигнала (свидетели, лица, споменати в сигнала, членове на семейството или лица, които могат да претърпят вреди или отмъщение в резултат на сигнала, както и тези, които предоставят правна, трудова или психологическа подкрепа).

Трябва да бъде включена и информация за помощниците и за информационните центрове (**вижте Глава 4** за повече подробности по този въпрос).

1.2.2. Материален обхват на сигнализирането

Прозрачност по отношение на материалния обхват. Препоръчително е да се посочи по отношение на кои области може или трябва да бъдат подавани сигнали, както и приложимите разпоредби²⁴. Освен това се препоръчва вътрешните и външните канали да имат точка за контакт за отправяне на запитвания, както и раздел с често задавани въпроси.

Няколко интервюирани експерти посочват, че в някои транспониращи закони има неясноти, предпоставки за неравно третиране или пропуски в защитата по отношение на няколко аспекта, включително за какво може или за какво не може да се подава сигнал²⁵. Тези пропуски в защитата могат да обезкуражат лицата, които потенциално биха подали сигнал за нередности. Например, съгласно Закон № 2/2023 в **Испания** лицата, сигнализиращи за нередности, нямат право на защита съгласно закона, ако става въпрос за леки нарушения, които не засягат въпросите, посочени в Директивата.

²⁴ Всъщност, според друг от интервюираните експерти, от решаващо значение е лицата да бъдат информирани за правната рамка и риска от съдебни дела.

²⁵ Например в Испания Закон № 2/2023 защитава и признава правата само на лицата, които сигнализират за: (а) престъпления, (б) тежки или много тежки административни нарушения и/или (в) нарушения на правото на Европейския съюз, засягащи финансовите интереси на Европейския съюз; по този начин са изключени например леки нарушения или случаи, които биха могли да допринесат за предотвратяване на по-сериозни престъпления. Някои от интервюираните експертите също така повдигнаха въпроса дали по реда за сигнализиране на нередности биха се приели за разглеждане сигнали за лоша администрация.

РАВЕНСТВО МЕЖДУ ПОЛОВЕТЕ

Прозрачност по отношение на материалния обхват. Препоръчително е да се посочат по отношение на кои области може или трябва да бъдат подавани сигнали, както и приложимите разпоредби⁵⁰. Освен това се препоръчва вътрешните и външните канали да имат точка за контакт за отправяне на запитвания, както и раздел с често задавани въпроси.

Случаите на злоупотреби с власт, основани на пола, като сексуален тормоз или сексуално изнудване, често са свързани с по-висок риск от отмъщение (вижте карето в [Глава 4](#)), което може да обезкуражи пострадалите да подадат сигнал. В някои случаи пострадалите може да не са сигурни дали такова неправомерно поведение попада в обхвата на законодателството за подаване на сигнали за нередности. Заинтересованите страни препоръчват изрично включването на тези въпроси в обхвата на подаване на сигнали за нередности. В България представители на гражданското общество подчертават, че ако възникнат проблеми, свързани с пола, на работното място, законодателството за подаване на сигнали за нередности трябва да се прилага заедно със съществуващите законови разпоредби срещу дискриминацията.

Препоръчва се:

- Законодателството на ЕС и националните стандарти относно насилието, основано на пола, да бъдат включени в механизмите за подаване на сигнали за нередности, за да се осигури цялостна защита. Да се разшири обхвата на защитата, за да се обхванат всички потенциални нарушения, злоупотреби и престъпления, включително сексуален тормоз и сексуално изнудване. Правната рамка за подаване на сигнали за нередности да вземе предвид основаната на пола дискриминация на работното място, в допълнение към приложимите правни разпоредби срещу дискриминацията и да предоставя подкрепа и защита на жертвите на сексуално изнудване и сексуален тормоз в рамките на законодателството за подаване на сигнали за нередности.
- Бъдещите международни, национални и местни регулаторни рамки да засилят мерките за създаване на адаптирани механизми за защита на жените, подаващи сигнали за нередности, и други уязвими групи, като гарантират, че каналите за подаване на сигнали са достъпни, приобщаващи и отговарят на техните специфични нужди и рискове.
- Да се разработят чувствителни към пола протоколи в рамките на регулациите на защита на лицата, сигнализиращи за нередности, които да се отнасят конкретно за случаите на сексуален тормоз, сексуално изнудване и други неправомерни действия, основани на пола. Да се интегрира принципът на прозрачност по отношение на правата и гаранциите на лицата, подаващи сигнали за нередности, с акцент върху чувствителната към пола комуникация и включването на маргинализираните групи. Ясната комуникация относно правата, гаранциите и органите, отговорни за обработката на сигналите, гарантира, че лицата, подаващи сигнали, се чувстват уверени в системата и разбират своята защита. Това включва ясни и достъпни насоки относно процедурите, възможностите за подкрепа и правната защита срещу ответни мерки с цел отмъщение.
- Да се подобри координацията с други служби за по-ефективно разглеждане на сигналите и предотвратяване на безнаказаността, вместо да се предполага, че случаите на сексуално изнудване могат да бъдат разследвани по-ефективно от други служби или механизми за подаване на жалби, като например тези, които се занимават със сексуално насилие.
- Да се предоставят конкретни примери за случаи, основани на пола, за да се повиши информираността и достъпността за лицата, които потенциално биха подали сигнали за нередности, като се укрепят техните права и наличните механизми за защита.
- Всяко лице следва да бъде информирано за правото си да сигнализира или разкрива нарушенията директно на съответните специализирани органи, като полицията, прокуратурата или съдилищата, особено в случаи на насилие, основано на пола. Това гарантира, че лицето е запознато с всички налични възможности за справяне с проблема и намиране на подходяща подкрепа. Споразуменията за обезщетение не трябва да изключват достъпа до съдебната система.
- Да се гарантира, че платформите за подаване на сигнали използват ясен, нетехнически език и предлагат канали на различни езици, включително жестомимичен език и други достъпни формати, за да са достъпни за разнообразен кръг лица, подаващи сигнали за нередности. Да се осигури използването на приобщаващ език по отношение на пола, като полът се направи видим, когато е необходимо, но се избягва ненужното му отбелязване, когато това не е от значение за комуникацията. Този подход насърчава яснотата, приобщаването и уважението към различните полови идентичности във всички форми на комуникация.
- Да се отчита въздействието на различията в степента на цифров достъп и да се осигурят алтернативни механизми за офлайн сигнализиране на разположение на лицата, които не разполагат със сигурен достъп до интернет, като се насърчава приобщаването за всички лица, независимо от техните способности за цифров достъп.

⁵⁰ Всъщност, според друг от интервюираните експерти, от решаващо значение е лицата да бъдат информирани за правната рамка и риска от съдебни дела.

КАКВО Е ПОЛОЖЕНИЕТО В НАЦИОНАЛНОТО ЗАКОНОДАТЕЛСТВО ЗА ПОДАВАНЕ НА СИГНАЛИ ЗА НЕРЕДНОСТИ?

ИТАЛИЯ

понятието за сексуален тормоз е релевантно от гледна точка на антидискриминационното законодателство. През 2006 г. Италия прие така наречения Кодекс за равни възможности за мъжете и жените (Законодателен указ № 198/2006), който дава определение за сексуален тормоз. При липсата на законодателство за подаване на сигнали за нередности, обхващащо сексуалния тормоз на работното място, прилагането на вътрешни процедури, които позволяват на служителите да съобщават за тормоз или друго сексуално посегателство, е оставено на преценката и желанието на работодателите.

ИСПАНИЯ

Законът за подаване на сигнали за нередности № 2/2023 (*Закон № 2/2023 от 20 февруари 2023 г. уреждащ защитата на лицата, които съобщават за нарушения на нормативната уредба, и борбата с корупцията*) не разглежда изрично насилието, основано на пола. Въпреки това, законът се прилага в условията на призната нормативна рамка за равенство, недискриминация и превенция на насилието, основано на пола, както и на национални планове и специфични публични политики по тази тема. Заслужава да се споменат три ключови момента:

- A* Материалният обхват на закона надхвърля европейските изисквания, като се прилага както за наказателни, така и за административни нарушения, включително нарушения на националното законодателство. Това позволява създаване на механизми за сигнализиране за всякакви престъпления, свързани с насилие, основано на пола.
- B* Въпреки че законът не изключва включването на този въпрос в съответните разпоредби или протоколи, защитата, основана на пола, е напълно съвместима с правната рамка за подаване на сигнали за нередности. И двете не само трябва да бъдат интегрирани в правната рамка за насилието, основано на пола, но законът за подаване на сигнали за нередности включва и защита за работниците, които съобщават за всякаква форма на злоупотреба или нарушаване на тяхното достойнство, здраве и безопасност. Следователно защитата и гаранциите трябва да обхващат всяко нарушение на физическата или психологическата неприкосновеност, включително всяка форма на дискриминация, основана на пола, или сексуално насилие.
- C* Кралският указ за създаване на Независим орган за защита на лицата, подаващи сигнали за нередности (A.A.I.) изисква балансирано представителство на половете в рамките на Консултативната комисия, създавайки полезен прецедент, който може да бъде възприет и от други национални или местни органи.

БЪЛГАРИЯ

Сексуалният тормоз не е обхванат от националния Закон за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения. Съществува обаче мнение, че ако тормозът се случва в работен контекст и застрашава обществен интерес, сигналът за това може да се счита за сигнал за нередност и на подателя да бъде предоставена съответната защита.

1.2.3 Прозрачност по отношение на основните принципи²⁶ на процедурата по администриране

Субектите **трябва ясно да определят** основните принципи на процедурата за подаване на сигнали за нередности, включително нейната цел, управление и рамка за съответствие. В **Испания**, например, тези принципи трябва да бъдат изрично отразени в политиката за вътрешната информационна система²⁷. Предоставянето на адекватна информация в този раздел е от **решаващо значение, за да се информират лицата** защо съществува каналът за сигнализиране, като се насърчи правилното и се предотврати неправилното използване на системата.

- Що се отнася до **сигурността**, от съществено значение е да се предостави информация за технологичните характеристики на сървъра или платформата и въведените мерки за информационна сигурност, за да се гарантира сигурна цифрова среда за лицата, сигнализиращи за нередности, а именно: криптиране, псевдонимизация, кодиране, черни кутии, контрол на достъпа, протоколи за сигурна връзка, двустепенно удостоверяване, правила за валидиране, подходящи описания на защитните стени, изчерпателни описания на характеристиките на сървъра/софтуера, CSRF символ и др.
- По отношение на **имунитета** е необходимо да се предостави ясна информация за обхвата на защитата на лицата, сигнализиращи за нередности, условията за достъп до защита съгласно закона и изрично да се гарантира, че няма да има репресии срещу лицата, сигнализиращи за нередности, ако сигналите са обосновани. Важно е да се подчертае, че защитата трябва да бъде гарантирана, дори ако сигналът не е обоснован, но лицето, подало сигнал, основателно вярва, че той е достоверен.
- Що се отнася до **поверителността**, трябва да се предостави ясно и просто обяснение как се гарантира поверителността на лицето, сигнализиращо за нередности, а именно: гарантиране на принципа на минимален достъп и цялост на данните, обяснение/обосновка на обработването на данните, описание на обработката на данните по време на всички етапи на процеса, време на съхранение и местоположение на информацията, данни и мерки за защита на самоличността на лицата, сигнализиращи за нередности, описание на системите за анонимизация и псевдонимизация, описание на контрола, наблюдението и отделянето на файловете на лицата, сигнализиращи за нередности, от останалите файлове, мерки за предотвратяване на повторна идентификация; а в случай, че каналът или част от процеса е възложен на външни изпълнители, е важно да се опишат всички мерки за сигурност, прилагани от доставчика и сървъра.
- По отношение на **анонимността** е важно каналите за подаване на сигнали да са разработени по такъв начин, че да позволяват, ако подателят на сигнала желае, да подава съобщения напълно анонимно, без да се компрометира самоличността му на който и да

²⁶ Чл. 5.2. з) от испански Закон № 2/2023, чл. 13 от българския закон, чл. 4, 5, 7 и 8 от италианския Законодателен указ № 24/2023 за транспониране на Директива 2019/1937/ЕС.

²⁷ Във връзка с това, вж. глава 2.

е етап от процеса. Въпреки това следва да се подчертае, че Директивата не признава анонимността като защитено право сама по себе си, а оставя на държавите членки да приемат и обработват анонимни сигнали в съответствие с националното си законодателство. Ето защо, въпреки че анонимността не е пряко гарантирана от Директивата, нейното доброволно включване в системите за докладване е добра практика.

Ако сигнализиращото лице се идентифицира в канала или системата, **поверителността** гарантира, че самоличността му няма да бъде разкрита на неупълномощени лица. Системите за сигурност (обикновено чрез криптиране, контрол на достъпа и т.н.) могат да бъдат полезни за запазване на поверителността, но трябва да се разработят вътрешни политики за подаване на сигнали за нередности, които подробно описват режима на поверителност и ролите на отговорните лица, за да се гарантира, че самоличността на лицата, сигнализиращи за нередности, остава защитена.

Анонимността, от друга страна, следва да гарантира, че лицето, което иска да запази самоличността си в тайна, може да бъде сигурно, че това ще стане, следователно в този случай самоличността на лицето не трябва да може да бъде свързана с неговите действия, устройства, данни или IP адреси, като се гарантира липсата на проследимост на самоличността на лицето, сигнализиращо за нередности (например чрез TOR системи или доказателства с нулево знание).

Според някои от заинтересованите страни съществуват редица пощенски кутии или канали на публични институции²⁸, които твърдят, че гарантират анонимност, но на практика това не е така.

1.2.4 Получаващи, администриращи и разследващи органи

Важно е да се гарантира прозрачност както по отношение на **приемащия орган** и **администриращия орган** (ако са отделни), така и по отношение на **разследващия орган** и **решаващия орган**. Това организационно разделение е от решаващо значение не само за повишаване на доверието в системата, но и за гарантиране на спазването на принципите на безпристрастност и независимост във всички разследвания, започнати в резултат на подадените сигнали.

Необходимо е също така да има **обяснение на въведените мерки** за предотвратяване на потенциални **конфликти на интереси** между органите или различните отдели и да се предвидят алтернативни варианти, ако сигналът засяга лицето, отговарящо за системата, или който и да е член на участващите органи (получаващите, администриращите, разследващите или решаващите органи, както евентуална втора или по-горна инстанция).

²⁸ Във връзка с това, вж. <https://xnet-x.net/es/proliferacion-buzones-anonimos-no-lo-son/>

1.2.5 Дати и срокове за потвърждение, допускане, разследване и решаване

Първи етап

Съгласно Директивата (член 9, параграф 1, буква б))²⁹, **потвърждение за получаване** на сигнала следва да бъде дадено на сигнализиращото лице в рамките на максимум седем календарни дни след получаването или регистрирането на сигнала, освен ако това може да застраши поверителността.

Срокове за допускане

Уебсайтът или вътрешната мрежа (интранет) трябва да посочват срока за извършване на предварително разследване или за вземане на решение по **допустимостта на сигнала**³⁰. Тази оценка предполага събиране на цялата необходима информация, документация и доказателства. Следователно субектите трябва да предоставят информация за следните аспекти:

- А. Максимален срок за провеждане на предварителна проверка за допустимост**, за да се избегнат неоправдани забавяния. Това не е предвидено в Директивата, нито в испанския Закон № 2/2023, българското или италианското законодателство, но испанският независим орган например, според Закон № 2/2023, разполага със срок от „не повече от десет работни дни от датата на регистриране на сигнала“, за да вземе решение дали да го допусне или отхвърли. Това може да се приеме за добър ориентир, като се вземат предвид характеристиките и капацитета на съответния субект, но при всички случаи е препоръчително публично да бъде предоставена ясна времева рамка, за да се избегнат неоправдани забавяния.
- В. Максимален срок за уведомяване на сигнализиращото лице за допускане до обработка или архивиране на сигнала.** Отново, нито Директива 2019/1937/ЕС, нито испанският Закон № 2/2023, българският или италианският закон, ясно уреждат този аспект. Испанският закон, например, установява максимален срок за уведомяване от „пет работни дни“, но не уточнява от кога трябва да се броят тези дни.

Според нас този **срок следва да тече от момента на извършване на предварителната проверка за допустимост** (за която максималният срок за изпълнение, както беше посочено по-горе, би могъл да бъде десет работни дни от датата на регистрацията³¹), освен ако сигналът не е анонимен или сигнализиращото лице не се е отказало от правото си да получава уведомления.

²⁹ Чл. 9.2, буква в) от испанския закон № 2/2023, чл. 16, т. 1 и чл. 23, ал. 1, т. 1 от българския закон, чл. 5, буква а) и чл. 7.3 от италианския закон, съответно за вътрешни и външни канали, като е установен и срок от седем дни за издаване на разписката за сигнала.

³⁰ Във връзка с това вж. Martínez García, D. (2021). *Anonymity, Pseudonymity, and Confidentiality: Towards a Comprehensive and Coherent Framework for the Protection of Whistleblowers* [Анонимност, псевдонимност и поверителност: към всеобхватна и съгласувана рамка за защита на лицата, подаващи сигнали за нередности].

³¹ Например, ако проверката за допустимост приключи на осмия работен ден след регистрацията на сигнала, субектът ще разполага с пет допълнителни работни дни от този момент, за да уведоми сигнализиращото лице, дали сигналът му е допуснат, което прави общо тринадесет работни дни от регистрацията на сигнала.

Друг важен аспект, който трябва да се вземе предвид, е, че съгласно испанския Закон № 2/2023 всички тези срокове за обработка или архивиране на сигнали се отнасят изключително до лицето, сигнализиращо за нередности. Нито в Директивата, нито в националното законодателство се определят ясни срокове за уведомяване за засегнатото лице на този процесуален етап. Това повдига въпроси дали засегнатото лице има право да бъде уведомено за подаване на сигнал, който не е преминал предварителната проверка за допустимост.

По-широкият прочит на член 18.2, буква а), т. 4 от испанския Закон № 2/2023 дава основание да се заключи, че такова уведомление е ненужно, тъй като установява като основание за недопустимост липсата на **нова или съществена информация** в сравнение с предишно съобщение, „във връзка с което са приключени съответните процедури“.

Това обаче е процедурно двусмислена формула, защото:

- Използването на процедури в множествено число означава, че може да става въпрос и за сигнал, който вече е архивиран³², защото не е преминал **проверката за допустимост**, за който обаче впоследствие е подаден допълнителен сигнал, предоставящ релевантни, значими или решаващи нови доказателства³³. Това повдига въпроса за максималния срок, в който могат да се съхраняват лични данни от архивирани сигнали³⁴. Например съгласно член 32.3 от **испанския закон**, ако сигналът е недопустим на основанията, посочено в член 18.2, буква а), т. 1 (липса на правдоподобност) и се докаже, че предоставената информация или част от нея не е вярна, „той се заличава незабавно, след като това обстоятелство бъде потвърдено, освен ако невярната информация може да представлява престъпление, в който случай информацията се съхранява за необходимия период, през който тече съдебно производство“, но във всички случаи не повече от три месеца, освен ако целта на съхраняването е да се предоставят доказателства за работата на системата³⁵, като в този случай информацията винаги трябва да се съхранява анонимизирано.
- Може да се отнася и до случаи, при които, след като е взето решение, че засегнатото лице няма да бъде уведомено преди **фазата на изслушване** поради риск от **унищожаване, укриване или промяна на доказателства** (член 19.2 от испанския Закон № 2/2023), сигнализиращото лице е предоставило допълнителна информация (съгласно член 18.2, буква а), т. 4 от закона), включително нови обвинения срещу засегнатото лице. В такива случаи, с изключение на хипотезата на риск от укриване, унищожаване или промяна на доказателства, свързани с тези нови обвинения, засегнатото лице следва да бъде уведомено съгласно обичайната процедура, за да се избегне потенциално накърняване на правото му на защита.

³² Всяко уведомление относно архивирането на сигнала трябва да бъде достатъчно мотивирано.

³³ При условие, че тези нови доказателства не са получени незаконно или в нарушение на основни права или свободи.

³⁴ В тази връзка вж. глава 3.

³⁵ Тази възможност повдига въпроса за потенциалната възможност за неограничено възобновяване на дела, архивирани по време на фазата на предварителна оценка, което пък създава предпоставки за възможно нарушаване на принципа *non bis in idem*.

Крайни срокове за процеса по разследване

По отношение на **сроковете за разследване**, въпреки че в **Директивата и националните закони** се посочва, че засегнатото лице се уведомява за подадения сигнал, както и за фактите, описани в него, няма установена ясна времева рамка за това. В това отношение може да се вземе предвид, че задължението за информиране на засегнатите лица за подаден сигнал срещу тях следва да се преценява с оглед на възможността за отмъщение и идентифициране на лицето, подало сигнала. Засегнатите лица трябва да бъдат информирани, когато има нужда да се защитят, например в случаи на предполагаеми ответни мерки за отмъщение, но не непременно след получаване на сигнала.

Субектите трябва да установят тези срокове в рамките на вътрешните си политики, за да гарантират защитата на процесуалните права на засегнатото лице. Това включва гарантиране на правото им да бъдат адекватно информирани за твърденията срещу тях, както и за всички значителни промени в обхвата на разследването и твърдените факти в съответствие с член 118.1, буква а) от испанския Наказателно-процесуален кодекс. В тази връзка в Наказателно-процесуалния кодекс изрично се посочва, че „тази информация се предоставя достатъчно подробно, за да позволи ефективното упражняване на правото на защита“. Това означава, че гарантирането на това право изисква информацията да съдържа не само кратко обобщение на фактите, но да е достатъчно подробна, за да се осигури ефективна защита.

Авторите на това ръководство считат, че след като бъде взето решение за допускане на сигнала за разглеждане, за засегнатото лице следва да се прилага същият максимален срок за уведомяване, както и за лицето, подало сигнала (като във всеки случай този срок не трябва да е подълъг): в срок от пет работни дни след решението за допускане на сигнала за разглеждане, засегнатото лице трябва да бъде уведомено, че срещу него е получен сигнал, който е допуснат за разглеждане и по който има започнало разследване³⁶. Ако обаче разследващият орган прецени, че уведомяването на засегнатото лице може да доведе до висок риск от укриване, унищожаване или промяна на доказателства от страна на самото засегнато лице или от трети лица, тази информация може да бъде предоставена на засегнатото лице по време на фазата на изслушване³⁷.

Срокове за решение

Що се отнася до сроковете за постановяване на решение, лицата трябва ясно и прозрачно да се информират, че максималното време за отговор³⁸ не може да надвишава три месеца от получаването на

³⁶ Всичко това се основава на член 118.5 от испанския Наказателно-процесуален кодекс (LECrim), който гласи, че: „Приемането на сигнал или жалба и всяко процесуално действие, което води до обвинение в престъпление срещу конкретно лице или лица, трябва незабавно да бъде доведено до знанието на предполагаемите отговорни страни“.

³⁷ Съгласно чл. 19.2 от испанския Закон № 2/2023, чл. 16 от българския закон.

³⁸ Съгласно чл. 9.2, буква г) от испанския Закон № 2/2023, чл. 16 (за вътрешните канали) и чл. 23 (за външния канал) от българския закон, и чл. 5 (за вътрешния канал) и чл. 8 (за външния канал) от италианския закон.

сигнала, освен в случаите на особена сложност, които изискват удължаване с максимум три допълнителни месеца.

1.2.6 Приложим дисциплинарен режим

Информация следва да бъде предоставено и за прозрачността по отношение на приложимите дисциплинарни мерки и последиците от умишлено съобщаване на невярна или подвеждаща информация. Както вече беше споменато в тази глава, необходимо е правилно да се предостави информация за крайната цел на канала, за да се предотврати неправилното му използване.

За тази цел е препоръчително лицата, които съзнателно **предоставят невярна информация**, като приписват неверни факти на друго лице, които, ако са верни, **биха представлявали нарушение, или невярно твърдят, че са жертва** на несъществуващо нарушение, трябва да бъдат информирани, че според някои законодателства те извършват **престъпление (чл. 456 от испанския Наказателен кодекс), а според други подлежат на строги административни санкции (например по италианското законодателство)**. В **Италия** законът предвижда административни санкции срещу лица, подаващи сигнали за нередности, които съзнателно подават фалшиви сигнали. Субектите трябва да докладват за такива случаи на съответните органи и да предприемат съответните действия.

1.2.7 Данни за контакт на външните канали

Данните за контакт на **външните официални канали**³⁹ са: електронният и пощенският адрес и телефонните номера, свързани с тези канали, данните за контакт на независимия орган⁴⁰ и други компетентни органи за получаване на такива сигнали, наличните възможности за обжалване и процедурите за защита срещу ответни действия с цел отмъщение, както и условията за получаване на правни, трудови, психологически и финансови съвети и подкрепа (в случай, че такива са предвидени).

³⁹ Раздел III от испанския Закон № 2/2023, чл. 21 от българския закон и чл. 9 (за външния канал, управляван от ANAC) от италианския закон.

⁴⁰ В Испания – Независимият орган за защита на лицата, подаващи сигнали за нередности (A.A.I.), в Италия – Националният орган за борба с корупцията (ANAC), в България – Комисията за защита на личните данни (CPDP).

ОТВОРЕНО УПРАВЛЕНИЕ

Заинтересованите страни от всички сектори предполагат, че **подход на сътрудничество**, включващ организациите на гражданското общество и публичните органи, **може да подобри информационните страници и системите за докладване за по-голяма яснота, като същевременно гарантира перспектива, ориентирана към лицата, сигнализиращи за нередности**. Това означава процедурите за сигнализиране да бъдат направени достъпни и лесни за разбиране.

В съответствие с това, организациите на гражданското общество предлагат прости, но ефективни стратегии за подобряване на използваемостта на съдържанието и повишаване на доверието в каналите за подаване на сигнали:

- да се използва опростен език, който е лесен за разбиране, като се избягва техническия или правния жаргон;
- да се дават практически примери, когато е възможно;
- да се повтарят ключовите инструкции за подаване на сигнали по време на целия процес на подаване, включително на информационната страница и в самия канал за подаване на сигнали;
- в платформата или формуляра за подаване на сигнали първо да се иска информация за предмета на сигнала, а накрая – за името на сигнализиращото лице.

За да се усъвършенстват системите за сигнализиране и информационните страници, е препоръчително да се провеждат **обществени консултации, отворени за всички заинтересовани страни, които могат да спомогнат за подобряване на съдържанието и използваемостта**, като същевременно насърчават сигнализирането. Компетентният орган следва да води тези консултации, като дава пример на другите задължени субекти да възпроизведат тези усилия или да провеждат свои собствените обществени консултации.

Добрите практики в областта на отвореното управление включват **предоставяне на ясна информация на интернет страниците на публичните органи относно подкрепата на лицата, сигнализиращи за нередности, и услугите по консултиране**, предоставяни от институциите (напр. омбудсмана) и гражданските организации. Такава разпоредба не е изрично предвидена от Директивата. Въпреки това, тъй като Директивата определя само минимални стандарти, държавите от ЕС, които желаят да не се ограничават с нейните изисквания и да включат такава разпоредба в националните си закони или подзаконови актове, заслужават да бъдат насърчени да го направят.

Например **Петият национален план за действие за отворено управление на Италия (2021-2023 г.)⁴¹** е съсредоточен върху засилване на сътрудничеството между институциите и гражданското общество в подкрепа на лицата, подаващи сигнали за нередности, и за повишаване на осведомеността.

Основните резултати включват:

- **Насърчаване на видимостта и достъпността на услугите за подкрепа, предоставяни от организациите на гражданското общество.** Националният орган за борба с корупцията (ANAC) ръководи работна група, включваща гражданското общество и публичната администрация, имаща за задача да идентифицира практики за подобряване на стандартите за защита на лицата, подаващи сигнали за нередности, и качеството на сигналите. Чрез поредица от съвместни инициативи с ANAC приносът на организациите на гражданското общество беше интегриран в законодателния процес по транспониране на Директивата, което доведе до публикуването на публичен списък на организациите, подкрепящи сигнализиращите лица, на уебсайта на ANAC. По

⁴¹ Виж също: <https://www.opengovpartnership.org/members/italy/>

този начин лицата, които потенциално биха подали сигнали за нередности и които посетят интернет страницата на ANAC, за да се запознаят с процедурите за подаване на сигнали и свързаните с тях предпазни мерки, веднага се запознават и с услугите за подкрепа, предназначени за тях. Тази мярка имаше вълнообразен ефект и други италиански публични администрации на свой ред възприеха добрата практика за повишаване на видимостта на услугите на гражданското общество чрез предоставяне на директна връзка към тях на своите уебсайтове.

- **Укрепване на капацитета на държавните служители чрез „общност на практикуващите“.** Под ръководството на Националното училище по администрация (SNA) беше създадена „общност на практикуващите“, включваща институциите, официално ангажирани с превенция на корупцията в италианските публични администрации. Тя представлява пространство за сътрудничество, където служителите в публичните администрации могат да обменят знания, да споделят добри практики и да повишават капацитета си за превенция на корупцията в своите организации. За да се повиши капацитетът на държавните служители да обработват сигнали за нередности и осведомеността им относно подаването на сигнали, общността на практикуващите проведе 14 сесии по теми, свързани с подаването на сигнали, като надхвърли първоначално определените цели за брой участници. Публикуван е изчерпателен наръчник, който да насочва практикуващите⁴², и са разработени три добри практики относно подаването на сигнали⁴³. Обучителните материали и практическите насоки са от жизненоважно значение за разпространяване на информацията относно системите за сигнализиране в и извън публичните администрации.

За да се увеличи ангажираността с механизмите за подаване на сигнали за нередности, всички задължени субекти могат да насърчават обучението на своите ръководители и служители. Според опита на организациите на гражданското общество **обучението, насочено към участници от всички сектори**, следва да се отдалечи от подхода, ориентиран към законодателството, и вместо това **да възприеме подход, основан на етична дилема**. Чрез тази методология, която е по-скоро експериментална, отколкото теоретична, участниците разсъждават върху сценарии на неправомерно поведение, като работят както индивидуално, така и в групи, за да идентифицират възможни решения, включително подаване на сигнал за нередности, което им помага да възпроизведат подаването на такъв сигнал. Модулите за обучение могат да бъдат организирани в съвместна форма, като включват институции и други заинтересовани страни, както в примера с проекта „Насърчаване подаването на сигнали: Защита на лицата, сигнализиращи за нередности чрез прозрачност, сътрудничество и стратегии за отворено управление“ (OPWHI).

Други инициативи в унисон с принципите на отвореното управление, като принципите за прозрачност и сътрудничество, могат да бъдат насърчаване на **съвместни комуникационни кампании** между различни заинтересовани страни, следвайки примера на OPWHI, или използване на националните медии за излъчване за комуникационни проекти със социална насоченост. Популярните платформи, като тези, свързани със спортни или културни събития, предоставят възможности за достъп до много широка аудитория

⁴² Виж също: <https://sna.gov.it/wp-content/uploads/2024/09/WHISTLEBLOWING-cultura-integrita.pdf>

⁴³ Първата подчертава необходимостта да се разглеждат лицата, подаващи сигнали за нередности, като човешка антикорупционна мярка; втората се фокусира върху разработването на политики, които третираят подаването на сигнали като дълг, а не като рискова дейност, за да се премахне социалната стигма и да се нормализира действието по сигнализиране; третата подчертава ролята на организациите на гражданското общество, като предоставя директна връзка към техните уебсайтове на платформата за подаване на сигнали (<https://sna.gov.it/home/attivita/comunita-di-pratica/comunita-di-pratica-per-rpct/buone-pratiche/whistleblowing-buone-pratiche/>).

1.3 ПРОЗРАЧНОСТ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ И КАНАЛИ: ФОРМАЛНИ ИЗИСКВАНИЯ

По отношение на формалните изисквания следва да се отбележи, че не е достатъчно просто да се предостави информация и данни за всички аспекти, описани по-горе. По-скоро тази информация трябва да отговаря на редица принципи и формални изисквания. Това означава, че тя трябва да бъде предоставена по **ясен, верен, пълен и достъпен начин**.

Например в испанския Закон № 2/2023 изрично се посочва, че съответната информация трябва да се предоставя по ясен и лесно достъпен начин и че: „Ако има уебсайт, тази информация трябва да се появява на началната страница, в отделен и лесно разпознаваем раздел.“

Освен това достъпът трябва да бъде **универсален**, което означава, че всички потенциални потребители трябва да имат равни възможности за достъп до информацията. Това изисква приемане на приобщаващи методи за всички хора. Според **Световната здравна организация (СЗО)** повече от един милиард души по света имат някаква форма на увреждане и от тях близо 200 милиона изпитват значителни затруднения в ежедневно си функциониране⁴⁴. Най-често срещаните видове увреждания обикновено са **зрителни, слухови, двигателни и когнитивни**.

В тази връзка в **Испания**, например, трябва да се вземат предвид както Кралски указ № 1112/2018 от 7 септември 2018 г. относно достъпността на уебсайтовете и мобилните приложения в публичния сектор, така и Насоките за достъпност на уеб съдържанието (WCAG), разработени от World Wide Web Consortium (W3C). По подобен начин в **Италия**⁴⁵ Законодателен декрет № 76/2020 за изменение на Закон № 4/2004 с въвеждането на параграф 1а в член 3 разшири прилагането на задълженията за достъпност, така че да се обхванат частни субекти, в допълнение към уебсайтовете в общественния сектор, които вече трябва да бъдат достъпни.

В съответствие с тези насоки е важно да се избягват определени практики при поддържането на интернет страници, като например поставяне на елементи за „кликване“ много близо един до друг или използване на много малки икони или текстови връзки с прекалено малък размер на шрифта. Също така е препоръчително да се познават правилните контрасти между цветовете комбинации между фона и текста. В този смисъл WCAG определя в критерий 1.4.3 параметрите, които трябва да се спазват при установяване на цветовия контраст⁴⁶.

⁴⁴ Данните са взети от <https://www.paho.org/es/noticias/5-12-2011-mil-millones-personas-viven-con-discapacidades#:~:text=M%C3%A1s%20de%20mil%20millones%20de,pues%20su%20prevalencia%20est%C3%A1%20aumentando>

⁴⁵ За допълнителна информация, вж. <https://www.agid.gov.it/ambiti-intervento/accessibilita-usabilita>

⁴⁶ Например за ниво AA се изисква контрастно съотношение между фона и текста от 4,5:1.

На последно място, за да се улеснят **разбираемостта** и **достъпността**, е препоръчително да се създадат раздели с често задавани въпроси или информационни видеоклипове, които обясняват основните аспекти от функционирането на канала за подаване на сигнали. Освен това, когато на потребителите се предоставят мултимедийни или аудиовизуални материали, те трябва да включват субтитри, аудио транскрипции и видео описания, за да се осигури достъпа до тях за лица с увреден слух.

1.4 ПРОЗРАЧНОСТ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ И КАНАЛИ: ГОДИШНИ ДОКЛАДИ И СТАТИСТИКА

Редовното публикуване на данни за ефективността на системата в годишните доклади служи като упражнение за **добро управление** и **отчетност**, а също така е начин за изграждане на доверие.

Като добра практика се препоръчва да се предоставя **статистическа информация на обществеността и заинтересованите страни** най-малко веднъж годишно в следните области:

- брой и типология на получените сигнали;
- брой сигнали, приети за обработка;
- брой сигнали, отхвърлени след извършване на проверка за допустимост;
- брой разследвани сигнали, завършили с решение;
- брой разследвани сигнали, довели до приемането на мерки, насочени към намаляване или избягване на установените рискови фактори;
- брой разследвани сигнали, които в крайна сметка са архивирани;
- брой наложени санкции или образувани дисциплинарни производства;
- брой случаи, в които субектът е сезирал прокуратурата, Европейската прокуратура, независимите органи или съдилищата;
- брой проведени обучения или семинари за служители и ръководители относно канала за сигнализиране;
- брой поверителни сигнали и брой анонимни сигнали;
- брой и типология на отправените запитвания;
- брой случаи, в които субектът е ангажирал услугите на външна компания за извършване на действия по разследването или предоставяне на експерти по криминалистика;
- брой и типология на мерките за подкрепа⁴⁷ или други мерки, предоставени доброволно;
- в случай на организация с международно присъствие: брой получени сигнали по географски райони;
- брой и типология на подобренията, направени в информационната система и канала;
- общи резултати по отношение на нивото на удовлетвореност,

⁴⁷ Описано в член 37 от испанския Закон № 2/2023, чл. 35 от българския закон, чл. 18 от италианския законодателен указ.

осведоменост и разбиране на системата сред нейните потребители.

Следва да се отбележи, че тези доклади или годишни отчети **не трябва да включват никакви лични данни**, особено данни, които биха позволили идентифицирането или повторното идентифициране на лица, подаващи сигнали за нередности, засегнати лица, свидетели или трети страни, участващи в различните процедури, дори ако тези данни вече са публикувани в резултат на окончателно решение.

1.5 ВЪТРЕШНА И ВЪНШНА КОМУНИКАЦИЯ ЗА ПОВИШАВАНЕ НА ОСВЕДОМЕНОСТТА

Системите за подаване на сигнали изискват добре разработени комуникационни стратегии, за да се гарантира тяхната достъпност и да се изгради доверие сред лицата, подаващи сигнали за нередности. Въпреки това продължават да съществуват няколко предизвикателства, като например непознаване на каналите за подаване на сигнали, негативното отношение към лицата, подаващи сигнали за нередности, в някои култури, страха от отмъщение и липсата на ефективни кампании за повишаване на осведомеността.

1.5.1 Вътрешна комуникация: предизвикателства и добри практики

Липса на яснота и недостатъчно обучение

Проведените интервюта разкриват, че много служители не знаят как да докладват за нарушения, а вътрешните канали за подаване на сигнали остават недокументирани. За справяне с този проблем е препоръчително да се провеждат периодични обучения, да се включи информация за подаването на сигнали в програмите за въвеждане на новопостъпили служители и да се засилят вътрешните кампании, подчертаващи важността на подаването на сигнали. Като **добра практика** някои компании имат въведени QR кодове с ясни инструкции за улесняване на достъпа до канала за подаване на сигнали.

Недоверие и негативно отношение

В някои случаи подаването на сигнали все още се възприема като акт на предателство. Интервютата показват, че страхът е основната бариера, което прави критична промяната в наратива. За да се преодолее това, комуникационните стратегии трябва да се фокусират върху представянето на подаването на сигнали като право и етична отговорност, подкрепено от изявления на служители или лидери, които подчертават важността му.

Интеграция с политиките за етика и съответствие

Интервютата също така показват, че много компании нямат реален ангажимент за администриране на сигналите. За да се укрепят тези механизми, системите за подаване на сигнали за нередности трябва да бъдат включени в системите за вътрешен одит и за контрол на риска, като по този начин се гарантира интегрирането им в корпоративното управление.

1.5.2 Външна комуникация и ангажиране на заинтересованите страни

Липса на прозрачност и лоша публична комуникация

Много организации не успяват да комуникират ефективно относно своите системи за подаване на сигнали. Мярка за промяна на наратива може да бъде публикуването на статистика и истории за успех, за да се изгради доверие. Разпространението на лошо администрирани канали за подаване на сигнали по-скоро създава объркване, отколкото да насърчава тяхното използване. За да се подобри тази ситуация, се препоръчва:

- от една страна, да се предоставя информация по подходящ начин за всички елементи, описани във втория раздел на настоящата глава, по ясен, верен, пълен и достъпен начин, а от друга страна, да се публикуват годишни доклади, и
- да се разработят стратегически кампании за повишаване на осведомеността и ключови действия в сътрудничество с гражданското общество.

Роля на гражданското общество и медиите

Според интервюираните гражданското общество може да играе ключова роля за повишаване на прозрачността, тъй като понякога стигмата около подаването на сигнали за нередности продължава да засяга лицата, подаващи сигнали, и да ограничава тяхното участие. За да се преодолее този проблем, е необходимо да се създадат канали за диалог с медиите и неправителствените организации, за да се засили отчетността и да се разшири обхватът на механизмите за подаване на сигнали.

1.6 ПРЕПОРЪКИ

1. ПО-ГОЛЯМА ЯСНОТА

По-голямата яснота във вътрешните канали и процеси за подаване на сигнали е от решаващо значение.

2. ПРОМЯНА НА ВЪЗПРИЯТИЕТО

Промяната на отношението към подаването на сигнали за нередности като етичен инструмент е от ключово значение.

3. ОСИГУРЯВАНЕ НА ПРОЗРАЧНОСТ

Осигуряването на пълна и смислена прозрачност⁴⁸ е от решаващо значение за осигуряването на по-голямо доверие⁴⁹.

4. ВКЛЮЧВАЩИ СТРАТЕГИИ

Необходими са приобщаващи стратегии с перспектива за равенство между половете и защита на лицата, подаващи сигнали за нередности.

5. ОБУЧЕНИЕ

Нужно е **обучение** на служителите и гражданите, както и на лицата, отговорни за администрирането на системите за подаване на сигнали.

Укрепването на **прозрачността и комуникацията** ще спомогне за **създаването на ефективна, достъпна и надеждна култура на подаване на сигнали** за нередности, насърчавайки **почтеността в организациите**.

⁴⁸ Много е важно на интернет страниците да има обяснени стъпките, които лицата, подаващи сигнали за нередности, трябва да направят и какви са процедурите, техните права и задължения.

⁴⁹ Според един от интервюираните е важно администрациите да включат инструменти, ресурси и данни за контакт с организациите на гражданското общество, които подкрепят лицата, подаващи сигнали за нередности.



Правилно разследване и управление в рамките на вътрешните системи за подаване на сигнали за нередности



ГЛАВА 2

ПРАВИЛНО РАЗСЛЕДВАНЕ И УПРАВЛЕНИЕ В РАМКИТЕ НА ВЪТРЕШНИТЕ СИСТЕМИ ЗА ПОДАВАНЕ НА СИГНАЛИ ЗА НЕРЕДНОСТИ

ГЛАВА 2

2.1 ОСНОВНИ ПРИНЦИПИ ЗА ПРАВИЛНО РАЗСЛЕДВАНЕ

В рамките на мисията за запазване на обществения интерес правната рамка, определена от Директивата, зависи от условие, което е от решаващо значение за нейната ефективност: *доверието в системата*. Когато вътрешен сигнал попада в приложното поле на Директивата, може да бъде започнато вътрешно разследване, което трябва да спазва всички правни гаранции и да бъде надлежно проследено. Вътрешните и външните канали за подаване на сигнали трябва да осигуряват адекватни гаранции срещу потенциални *репресии*, което представлява крайъгълен камък за насърчаване на сигнализиращите лица да излязат и да нарушат мълчанието.

Член 7, параграфи 1 и 2 от Директивата установяват принципа, че сигнализиращите лица са свободни да избират дали първо да сигнализират вътрешно или направо по външни канали. Външното сигнализиране се предвижда по-специално в ситуации, когато нарушението не може да бъде ефективно отстранено вътрешно или когато сигнализиращото лице счита, че има риск от ответни действия с цел отмъщение (вж. член 7, параграф 2). Няколко държави членки (които не са посочени в доклада) неправилно налагат задължение за вътрешно сигнализиране първо или разрешават пряко външно сигнализиране само при определени обстоятелства. Освен това някои държави членки не са предвидили изрично защита на лицата, подаващи сигнали пред институциите на ЕС. В този контекст вътрешното сигнализиране е най-подходящото средство за събиране на информация за ранно разрешаване на заплахи за обществения интерес. Поради тази причина се **дава предимство на вътрешните канали за подаване на сигнали**, въпреки че вътрешното сигнализиране не е задължително условие за подаване на външни сигнали.

На второто заседание на експертната група на Европейската комисия по Директивата⁵¹ се отбелязва, че когато лицата, сигнализиращи за нередности, подават сигнал директно по външни канали, организациите не са в състояние своевременно да отстранят ситуацията или нередността. Следователно организациите трябва да създадат ясни, лесно достъпни и ефективни вътрешни канали и да изграждат **корпоративна култура**, която активно насърчава вътрешното сигнализиране за нарушения. Вътрешните разследвания, произтичащи от сигнали или информация, получени по вътрешни канали, независимо дали в рамките на публична или частна организация, се провеждат в **обществен интерес**.

Вътрешните процедури за сигнализиране и последващите действия трябва да отговарят на определени основни изисквания, за да постигнат предвидената си цел и да са в съответствие с разпоредбите на Директивата и националното законодателство. Тези изисквания са по същество следните:

- Вътрешните канали трябва да позволяват на лицата, попадащи в персоналният обхват на Директивата, да докладват за нарушения, обхванати от нейния материален обхват и националните транспониращи закони.
- Каналите трябва да бъдат проектирани, създадени и администрирани сигурно, за да се гарантира конфиденциалността на самоличността на сигнализиращото лице и на всяка трета страна, посочена в сигнала, като същевременно се защитават личните данни от неоторизиран достъп.
- Потвърждение за получаване трябва да бъде изпратено на подателя в срок от седем дни от получаването на сигнала.
- По време на обработката на сигнала може да се поддържа комуникация с подателя и при необходимост може да бъде поискана допълнителна информация.
- Каналите трябва да позволяват надлежно проследяване и ефективна обработка на подадените сигнали, включително анонимни, когато е приложимо.
- Трябва да се предоставя ясна и достъпна информация относно външните канали, администрирани от компетентните национални органи и, когато е приложимо, от институциите или органите на ЕС.

⁵¹ Експертната група на Европейската комисия е консултативна група, съставена от експерти, представляващи държавите – членки на Европейския съюз, с отговорности за транспонирането на Директива 2019/1937/ЕС. Основната ѝ мисия е да изготвя препоръки към държавите членки за транспониране на Директива 2019/1937/ЕС.

РАВЕНСТВО МЕЖДУ ПОЛОВЕТЕ

Прилагането на чувствителни към аспектите на пола канали и целенасочени политики би повишило ефективността на процесите на подкрепа, особено за жените и други уязвими групи.

Конкретните препоръки за осигуряване на чувствителни към пола механизми за сигнализиране могат да включват:

- **Приобщаващ дизайн и представителство:** Гарантиране на участието на жените и лицата с различна полова идентичност в разработването на механизми и политики за сигнализиране.
- **Координация и протоколи, чувствителни към аспектите на пола:** Създаване на протоколи, основани на пола, за всеки вътрешен канал за подаване на сигнали. Координиране на усилията между механизмите за докладване, свързани с кодексите за поведение, механизмите за борба с корупцията и механизмите за докладване на насилие, основано на пола.
- **Чувствителни към равенството между половете системи за сигнализиране и разследване с цялостни услуги за подкрепа.** Ясни насоки за случаи, основани на пола, с обучен персонал, който да обработва сигналите деликатно. Информирание на лицата, подаващи сигнали за нередности, за външни услуги за подкрепа, като например правна помощ, психологическа подкрепа и организации за подкрепа на преживели насилие.
- **Често задавани въпроси и канали за подкрепа, чувствителни към пола.** Разработване на специален канал за запитвания, свързани с неправомерно поведение, основано на пола. Осигуряване на раздел „Често задавани въпроси“ или ясни насоки за подаване на сигнали по въпроси, свързани с пола.
- **Осведоменост и обучение.** Провеждане на обучение за осведоменост и повишаване на информираността относно равенството между половете, в организациите, които разполагат с канали за подаване на сигнали. Справяне със стереотипите и предубежденията, свързани с пола, за да се гарантира приобщаваща и ефективна система за подаване на сигнали за нередности.

2.2 ПРЕДИЗВИКАТЕЛСТВА ПРИ ВЪТРЕШНИТЕ РАЗСЛЕДВАНИЯ

Вътрешните разследвания **имат за цел да проверят истинността или правдоподобността на докладваните факти** и да идентифицират лицата, отговорни за въпросното нарушение или нередност. Особено важно е, както за валидността на самите вътрешни разследвания, така и за гарантиране на спазването на Директивата и националното законодателство, всички методи, използвани за събиране на доказателства, винаги да зачитат основните права.

За повече подробности относно защитата на основните права вижте [Глава 1](#).

Какви са предизвикателствата, които могат да възникнат по време на вътрешното разследване?

- Запазването на **поверителността** на личните данни може да бъде сложно и изисква прилагането на специфични технически, **организационни мерки и мерки за сигурност** (като ограничен и йерархичен достъп, двустепенно удостоверяване, вътрешна анонимизация и др.), изрично предназначени за тази цел. По време на **вътрешни разследвания** самоличността на сигнализиращото лице може да бъде разкрита или установена по невнимание, тъй като определени характеристики (напр. пол, длъжност, свързан проект и т.н.) могат косвено да разкрият неговата самоличност. Освен това искането на информация от други отдели или провеждането на лични интервюта може неизбежно да разшири **кръга от лица**, запознати с разследването и потенциално със самоличността на сигнализиращото лице.
- Гарантиране на **поверителността на самоличността на лицата, подаващи сигнали**, особено когато администрирането на вътрешните канали за подаване на сигнали е възложено на трета страна (подизпълнител). Това възлагане на дейности на външни изпълнители трябва да е в съответствие със **съображение 54 от Директивата на ЕС**, в което се посочва, че **трети страни** могат да бъдат външни доставчици на платформи за сигнализиране, външни съветници, одитори, представители на синдикални организации или представители на работниците и служителите. Възлагането на дейности на външни изпълнители по своята същност увеличава броя на лицата с достъп до чувствителна информация. Поради това **изричните гаранции за независимост** и поверителност трябва да бъдат ясно посочени в договорното споразумение между организацията и външната трета страна. Съгласно член 8, параграф 5 от Директивата в случай на нарушение отговорността споделят както третото лице, така и задълженият субект. **Експертите считат, че солидарната отговорност** е най-ефективният начин за защита на правата на лицата, сигнализиращи за нередности, като позволява на сигнализиращото лице да предприеме правни действия срещу субекта, външната трета страна или и двете.
- Експертите също така считат, че **обработването на данни за самоличността на лице, сигнализиращо за нередности**, представлява „обработване на лични данни“ по смисъла на Общия регламент относно защитата на данните (GDPR). Следователно **санкциите** за разкриване на самоличността на лицето, сигнализиращо за нередности, следва да бъдат по-строги от **санкциите**, които обикновено се предвиждат в националното законодателство за други **нарушения на поверителността на личните данни**. Тази повишена строгост е необходима, защото разкриването на самоличността на сигнализиращото лице **може да го изложи** на отмъщение и да отслаби доверието в самата система за подаване на сигнали.
- В някои случаи санкциите за нарушаване на поверителността се транспонират неправилно – например поради **липса на подходящи препратки** към приложимото законодателство. Тази ситуация е особено тревожна, първо, поради липсата на хармонизация на **европейските стандарти за защита**, и второ, защото подкопава един от крайъгълните камъни на европейското законодателство за защита на лицата, сигнализиращи за нередности.

- По време на вътрешните разследвания влияние оказват и частните интереси на организациите. Следователно в определен контекст вътрешните разследвания на нарушения и нередности могат да се разглеждат като механизми на **публично-частно сътрудничество**. Интервютата, проведени в **Италия**, обаче очертават конкретно предизвикателство: конфликти на интереси могат да възникнат, когато съдържанието на сигнала на лицето, сигнализиращо за нередности, противоречи на интересите на организацията.

ОТВОРЕНО УПРАВЛЕНИЕ

Ефективното разследване и администриране на системите за вътрешно сигнализиране изискват **прозрачност и ясно дефинирани насоки**, за да се гарантира последователност и справедливост в различните сектори, включително публичния сектор, частния сектор и организациите с нестопанска цел. Такива насоки могат да бъдат разработени чрез подход на съвместно проектиране (co-design), включващ публичните органи, отговарящи за получаването на сигнали за нередности, и други заинтересованите страни. Този процес на сътрудничество може да се осъществи чрез **диалози или обществени консултации**, както показва опита на италианския Национален орган за борба с корупцията (ANAC).

През 2024 г. ANAC стартира онлайн обществена консултация⁵², за да получи обратна връзка относно своя проект за насоки за подаване на сигнали за нередности. Целта е да се насърчи еднаквото и ефективно прилагане на законодателството за подаване на сигнали за нередности, като същевременно се намали несигурността, свързана с тълкуването, по отношение на субектите, администриращи вътрешни канали както в публични, така и в частни организации. Моделът ANAC предоставя полезна рамка, която други държави биха могли да възпроизведат, за да засилят ангажираността на заинтересованите страни в разработването на насоки за подаване на сигнали за нередности:

- открита процедура за онлайн консултация с продължителност най-малко един месец, за да се даде достатъчно време за обратна връзка;
- лесна за използване платформа за изпращане на становища (напр. онлайн въпросници);
- широко популяризиране на инициативата в множество подходящи форуми, за да се гарантира видимост и да се насърчи участието;
- персонализирани покани към ключови заинтересовани страни, активно участващи в процесите, свързани с подаването на сигнали за нередности.

Практикуващите юристи препоръчват да се определи специално **звено за контакт в рамките на публичния орган, отговорен за подаването на сигнали** за нередности. Това лице ще действа като помощник на администраторите на вътрешни канали за сигнализиране, предоставяйки насоки и разрешавайки предизвикателства при обработването на сигналите и разследванията. Освен това опасенията, свързани с правилното разследване на сигналите, могат да бъдат преодоляни чрез партньорски срещи между администраторите на вътрешни канали за подаване на сигнали и публичния орган. За да се насърчи сътрудничеството и непрекъснатото усъвършенстване, създаването на **работна група или общност на практикуващите** относно подаването на сигнали за нередности може да бъде включено в партньорството за открито управление, независимо дали като част от редовните национални планове за действие или като ангажимент за предизвикателство на отвореното управление.

⁵² Виж също: <https://www.anticorruzione.it/en/-/news/071124.lg.whistleblowing>

Друг ключов аспект, улесняващ правилното провеждане на разследванията, е гарантирането на високото качество на сигналите за нередности. Ефективен начин за създаване на силна вътрешна система за сигнализиране – такава, която е възможно най-точна и съобразена с действителните рискове, пред които е изправена организацията (независимо дали е публична или частна) – е да се извърши **оценка на риска от потенциално неправомерно поведение, което може да възникне чрез подаване на сигнали за нередности**.

В идеалния случай този процес трябва да включва множество отдели, области и сектори в рамките на организацията. Въпреки това, особено в случая на публичните институции, той може да се осъществи и чрез използване на принципите на отворено управление чрез ангажиране на гражданското общество в хода на процеса. Външният принос може да осигури по-широка перспектива и по-задълбочено разбиране на факторите, свързани със средата и контекста, помагайки на организацията да идентифицира рискове, които иначе биха могли да бъдат пренебрегнати или подценени. Резултатът от този процес е система за сигнализиране, която включва добре дефинирани сценарии, съобразени с по-задълбочено разбиране на рисковете за организацията. Това не само подпомага лицата, подаващи сигнали за нередности, при изготвянето на по-ясни и по-точни сигнали, но също така гарантира по-ефективно и задълбочено разследване.

2.3 ОБЩА РАМКА НА ПРОЦЕДУРИТЕ ПО РАЗСЛЕДВАНЕ

Член 9, параграф 1 от Директивата определя, че вътрешната процедура за подаване на сигнали трябва да включва **надлежащи последващи действия** от страна на лицето или службата, определени за тази цел (вижте **Глава 1** относно прозрачността в процедурата за подаване на сигнали за нередности).

Гл. 1 >

Във връзка с това член 5, параграф 12 от Директивата определя „последващи действия“ като:

„всяко действие, предприето от лицето, приемащо сигнал, или от компетентен орган, с цел оценка на точността на представените в сигнала твърдения и по целесъобразност с цел третиране на сигнализираното нарушение, включително чрез действия като вътрешна анкета, разследване, наказателно преследване, действия за обезпечаване на средства или приключване на процедурата.“

Директивата включва две действия в концепцията за **надлежно проследяване на сигнала**: оценка на точността на сигнализираните проблеми и разрешаване на сигнализираното нарушение.

Според **доклада за прилагането на Директивата** няколко компонента на тази разпоредба (член 9), като например задължението за надлежно

проследяване на сигналите, сроковете за изпращане на потвърждение за получаване и провеждането на присъствени заседания, не са правилно транспонирани в повечето държави членки. Националното законодателство за транспониране на Директивата като цяло установява **определено минимално съдържание и/или принципи** за вътрешните процедури за сигнализиране, въпреки че обикновено не ги урежда подробно. По този начин задължените субекти запазват известна свобода на преценка сами да уредят и организират вътрешните разследвания, при условие че спазват принципите и минималните изисквания, определени от националното законодателство. Това позволява процедурите да бъдат по-добре адаптирани към характеристиките на всяка организация.

В **Испания** **член 9.2** от **Закон № 2/2023** предвижда, че вътрешната процедура за подаване на сигнали трябва да отговаря на набор от минимални принципи и изисквания, включително ясно идентифициране на вътрешни и външни канали за подаване на сигнали, изпращане на потвърждение за получаване на сигнала в рамките на седем дни и определяне на максимален срок от три месеца за приключване на разследванията, който може да бъде удължен в сложни случаи. Освен това има задължение за осигуряване на непрекъсната комуникация с лицата, сигнализиращи за нередности, като се гарантира правото им да бъдат информирани за напредъка на разследването. Трябва да се гарантират и поверителността, презумпцията за невиновност, защитата на личните данни и зачитането на достойнството на засегнатите лица. Ако сигнализираните факти потенциално съставляват престъпление, информацията трябва да бъде препратена на прокуратурата или, ако са засегнати финансовите интереси на ЕС, на Европейската прокуратура.

Подобно изискване съществува и в **Италия**, където **член 4** от **Законодателен указ № 24/2023** определя, че както субектите от публичния, така и тези от частния сектор трябва да създадат канали, гарантиращи поверителността на самоличността на сигнализиращото лице, лицата, посочени или споменати в сигнала, както и съдържанието на сигнала и придружаващата го документация, включително чрез инструменти за криптиране.

Процедурите и протоколите, одобрени от задължените субекти, следва ясно да очертават общите принципи, уреждащи вътрешните канали за подаване на сигнали и защитата на лицата, подаващи сигнали за нередности в рамките на организацията. Тези процедури трябва да бъдат официално одобрени от административния или управителния орган на субекта. Освен това те трябва да бъдат публикувани и ефективно сведени до знанието на всички потенциални потребители на канала. Правилното разпространение на информацията е от съществено значение, тъй като помага за предотвратяване на злоупотреби с канала и намалява броя на подадените сигнали, които не могат да бъдат обработени по подходящ начин.

2.3.1 Процедура по разследване: насоки, принципи и гаранции

За да се **гарантира правна сигурност** при вътрешните разследвания и да се **защитят самите разследващи лица**, е **препоръчително вътрешните процедури** за администриране на сигналите да бъдат подробно и изчерпателно описани. Освен минималното съдържание и принципи, очертани от националните закони за транспониране на Директивата, вътрешните процедури **следва изрично да описват** всяка фаза от процеса на разглеждане на сигнала, като **посочват действията**, които трябва да бъдат извършени на всеки етап. Тези процедури следва да регулират и методите за проверка и да очертаят подходящи мерки за съхраняване и опазване на документацията и доказателствата, събрани по време на разследванията.

Етапите на вътрешната процедура за сигнализиране, които могат да бъдат включени в процедурата, са следните:

- фаза на получаване на сигнала;
- фаза на допускане или отхвърляне на сигнала;
- фаза на разследване;
- фаза на завършване или прекратяване на разследването.

2.4 ПРАВА НА СИГНАЛИЗИРАЩИТЕ ЛИЦА

Лицето, което подава сигнал, има **основното право** да подаде поверителен сигнал и да не разкрива самоличността си, когато това е разрешено от националното законодателство.

Анонимно подаване на сигнали

Директивата и националните законодателства за нейното транспониране установяват задължение за запазване на поверителността на самоличността на сигнализиращото лице и на съдържанието на сигнала. По отношение на анонимните сигнали Директивата позволява различни подходи на национално равнище, тъй като не всички държави членки приемат анонимно подаване на сигнали. Когато обаче това е разрешено, **трябва да се гарантира комуникацията с анонимно сигнализиращите лица**.

В **доклада за прилагането на Директивата**, публикуван от Европейската комисия, се подчертава, че ако държавите членки изискват от субектите да приемат анонимни сигнали, **тези сигнали трябва да се разглеждат при спазване на същите процесуални права като неанонимните сигнали**. Това включва както правата на сигнализиращото лице, така и задълженията на субектите и органите да извършват надлежни последващи действия.

Тъй като вътрешното разследване може да доведе до **дисциплинарно, административно-наказателно или наказателно производство**, доказателствата трябва да бъдат събрани в съответствие с приложимите закони и при спазване на процесуалните правила и правата на всички участващи страни. Те включват **основни права, трудови права, права, установени в Директивата и националното законодателство, както и вътрешните процедури и протоколи, одобрени от организацията**.

Препоръчителна **добра практика** е защитата на правата на подателите на сигнали чрез **солидарна отговорност**, като им се даде възможност да предприемат правни действия **срещу задължения субект, срещу външната трета страна, администрираща системата за сигнализиране, или срещу двете страни**.

Сигнализиращите лица имат право:

- да подадат сигнал устно или писмено;
- да изберат дали да подадат сигнал чрез вътрешния канал, освен ако нямат основателни причини да сигнализират външно;
- да получат поверителен и безплатен правен съвет по време на подаване на сигнала.

Съветът, който сигнализиращите лица имат право да получат, трябва да изясни

- дали сигнализираната информация попада в обхвата на правилата за защита на лицата, сигнализиращи за нередности;
- най-подходящия канал за подаване на сигнала;
- алтернативни процедури, в случай че информацията не попада в обхвата на разпоредбите за подаване на сигнали за нередности;
- наличните мерки за защита и подкрепа;
- получаването на потвърждение за получаване на сигнала;
- достъпа до мерки за защита и подкрепа, включително финансова помощ и психологическа подкрепа в определени случаи, при условие че лицето, сигнализиращо за нередности, отговаря на условията за защита; това включва и случаи, в които лицата са сигнализирали анонимно, но по-късно са били идентифицирани и са пострадали от ответни действия;
- правото да бъдат информирани за състоянието на своя сигнал и да получават актуална информация за резултатите от разследването;
- правото да запазят поверителността и да защитят самоличността си по време на целия процес;
- правото личните им данни да бъдат обработвани при спазване на правата, предоставени им от европейското законодателство и съответното национално законодателство.

В своите транспониращи закони държавите членки могат да **въведат разпоредби**, които са по-благоприятни за правата на лицата, сигнализиращи за нередности, от установените в Директивата. Важно е да се отбележи, че за да отговарят на условията за защита, сигнализиращите лица трябва не само да подават сигнали по каналите, предвидени в Директивата, но и да имат **разумни основания да смятат, че въз основа на информацията, с която разполагат към момента на подаване на сигнала, фактите, които разкриват, са верни**. Защитата **не се разпростира** върху злоупотреби, злонамерени или фалшиви сигнали.

Засегнатото лице трябва да има следните основни права:

- да запази самоличността си;
- да бъде информирано и изслушано по начин и в срок, които се считат за подходящи, за да се гарантира ефективността на разследването;
- да има достъп до съдържанието на материалите по преписката и да изразява мнение;
- да се спазва презумпцията за невиновност и правото на неприкосновеност на личността;
- да получава информация за предприетите мерки в резултат на разследването, които го засягат;
- личните му данни да бъдат обработвани в съответствие с правата, предоставени му от европейското законодателство и съответното национално законодателство.

Съгласно **съображение 76 от Директивата** държавите членки трябва да гарантират, че компетентните органи разполагат с **адекватни процедури** за защита при обработване на сигнали и за защита на личните данни на лицата, посочени в сигнала. **Тези процедури трябва да гарантират**, че поверителността на самоличността на всяко сигнализиращо лице и на всяко засегнато лице, но също така и на трети страни, посочени в сигнала, като свидетели или колеги, е защитена на всички етапи на процедурата.

2.4.1 Права, свързани с обработването на лични данни

По отношение на правата, свързани с **обработването на лични данни**, когато данните са получени от заинтересованата страна, трябва да се предостави информацията, посочена в чл. 13 от Регламент (ЕС) 2016/679.

Сигнализиращите лица, засегнатите лица, както и **третите лица**, посочени в сигналите и в разследванията, могат да упражняват правата, признати в членове 15-22 от Регламент (ЕС) 2016/679 (право на достъп на субекта на данните, право на коригиране, право на изтриване, право на ограничаване на обработването, задължение за уведомяване при коригирането или изтриването на лични данни или ограничаване на обработването, право на преносимост на данните, право на

възражение, право да не бъдат обект на вземане на автоматизирани индивидуални решения, включително профилиране).

В някои случаи обаче националните закони за транспониране на Директивата **ограничават упражняването на определени права**. Например, правото на възражение срещу обработването на лични данни от компетентните органи е ограничено в някои юрисдикции.

2.5 ВЪТРЕШНА СТРУКТУРА ЗА СИГНАЛИЗИРАНЕ И ОТГОВОРНОСТИ

Решението за **определяне на отговорно лице** за вътрешния канал за подаване на сигнали и, когато е приложимо, допълнителен персонал за администриране на процедурите за последващи действия във връзка със сигналите (както е установено в някои държави, като **Испания**) следва да се взема по прозрачен начин. Това означава, че потенциалните потребители на канала **трябва да бъдат информирани** за самоличността на тези лица. Лицата, отговорни за администрирането на вътрешния канал, **трябва да притежават необходимия технически опит**, както и уменията и компетенциите, необходими за ефективното провеждане на вътрешни разследвания. Това **изискване за прозрачност, обаче, създава и предизвикателства**, особено при създаването на ефективни комуникационни платформи за лица извън организацията (напр. подизпълнители, бивши стажанти и др.).

От практическа гледна точка, **особено в големите организации**, може да е невъзможно едно лице или отдел да **обработва всички вътрешни сигнали**, подадени чрез канала. Освен това член 16 от Директивата задължава държавите членки да **гарантират, че самоличността** на сигнализиращото лице не се разкрива без неговото изрично съгласие, освен на упълномощен член на персонала, отговарящ за разглеждането или проследяването на сигналите, както е определено в член 5, параграф 12 от Директивата. Тази разпоредба предполага, че **екип от лица** – с необходимото техническо обучение и обвързани със строги задължения за поверителност – **може да бъде ангажиран с наблюдението на сигналите**, анализирането на случаите от различни гледни точки или изпълнението на различни разследващи функции.

Ето защо **се препоръчва:**

- **да се направи изрично позоваване** на съществуването на канала за сигнализиране, в съответствие със задълженията за прозрачност, определени в Директивата на ЕС, в договорни клаузи или други допълнителни документи;
- **предварително да се определи** заместник на лицето, който може **временен или постоянно** да изпълнява функциите на отговорното лице, администриращо вътрешния канал за подаване на сигнали в случаи на напускане, отсъствие или заболяване; този **механизъм за заместване** е от съществено значение и в ситуации, в които **титularyният администратор на вътрешния канал за подаване на**

сигнали трябва да си направи отвод поради конфликт на интереси или други законово установени основания;

- **да бъдат напълно информирани всички лица, засегнати от сигнала, за процедурата по разследване и за самоличността на лицата, отговорни за провеждането на вътрешното разследване.**

Освен това засегнатите лица трябва да бъдат убедени, че посочените лица ще действат **обективно и безпристрастно**.

Като гарантират, че сигналите се обработват и разследват от безпристрастни и компетентни специалисти, организацията ще повишат доверието и ефективността във вътрешната система за сигнализиране. Това от своя страна ще засили доверието сред всички потенциални ползватели, че каналът за подаване на сигнали функционира правилно и надеждно и че сигналите се приемат сериозно и се обработват старателно. Наличието на такава разпоредба е от решаващо значение за гарантиране на обективност и безпристрастност при вътрешните разследвания.

2.5.1 Организационна структура на системите за вътрешно сигнализиране

Административният или управителният орган на задължения субект може да определи **лицето(ата), отговорно(и) за администрирането на вътрешния канал за подаване на сигнали** и за извършване на последващите действия по тях, какъвто е случаят съгласно **испанското** и **италианското** законодателство. За да бъде системата ефективна и надеждна, всички комуникации трябва да се управляват ефикасно и отговорно в самата организация. Тази отговорност може да падне върху лицето, което отговаря за вътрешния канал за подаване на сигнали. Ето защо е от съществено значение тези лица, поради позицията си в организацията, да могат да изпълняват задълженията си **независимо и автономно**, без да са обект на външно влияние, като разполагат с достъп до всички лични и материални ресурси, необходими за изпълнение на тяхната роля. Както беше споменато по-горе, специфичните особености на всяка организация могат да оправдаят възлагането на тази отговорност на екип, а не на конкретен човек. Освен преимуществото от колективното вземане на решения, такъв екип би могъл да внесе и мултидисциплинарна перспектива в разследванията.

Изборът на подходящи специалисти може да варира в зависимост от вида и структурата на организацията. Въпреки това, тези, които отговарят за администрирането на вътрешния канал за подаване на сигнали, трябва да се ангажират със спазването на нормативните изисквания, почтеността и етичните принципи и ценности на организацията. Това е така, защото тези лица трябва да изпълняват функциите си **независимо и автономно и във всеки случай да избягват конфликти на интереси**. В крайна сметка надеждността на

вътрешната система за сигнализиране **зависи от доверието, което служителите имат в лицата, отговарящи за обработката на сигналите**. Ако служителите смятат, че сигналите се администрират обективно и ефективно, те ще бъдат по-склонни да използват вътрешния канал.

В по-малките организации тази функция може да се изпълнява от изпълнителния ръководител, който е в добра позиция да **комуникира директно** с ръководството. Такива са например служителят, отговарящ за съответствието, специалистът по човешките ресурси, служителят, отговарящ за институционалния интегритет, служителят по правни въпроси или служителят по защитата на личните данни, ръководният финансов служител, одитора или членовете на съвета на директорите.

По принцип за лицето, отговарящо за вътрешния канал, може да възникнат задължения, произтичащи от администрирането и правилното функциониране на вътрешната система. Тези задължения могат да се отнасят до надлежното обработване и проследяване на сигналите, свързано с **гаранциите за защита** на подателя на сигнала в самата организация, както и с поведението му, когато трябва да взаимодейства с компетентните органи. Освен това в някои случаи отговорното лице може да понесе **наказателна отговорност**, ако поведението му съставлява престъпление според приложимото наказателно законодателство (например разкриване на тайни, престъпление по служба и др.).

Във всеки случай при определянето на специфичните задължения на отговорните лица и администраторите на вътрешния канал е необходимо да се вземат предвид задълженията, установени от националното законодателство на държавите членки, с което се транспонира Директивата.

2.5.2 Конфликти на интереси във вътрешните системи за сигнализиране

Конфликтите на интереси възникват в ситуации, в които безпристрастността и обективността на лицата, отговорни за вземането на професионално решение, са компрометирани от личен или външен интерес. Както всички рискове, конфликтите на интереси могат и трябва да се управляват проактивно. За да се гарантира справедливост и надеждност, вътрешните процедури за администриране на сигналите трябва изрично да включват мерки за идентифициране, управление и справяне с конфликти на интереси, които могат да засегнат лицата, отговорни за обработката и разследването на сигналите.

Това гарантира, че лицата, провеждащи вътрешни разследвания, остават безпристрастни и обективни.

Моделът, базиран на реакцията към конфликтите на интереси - изчакване, докато конфликтът възникне, преди да се вземе решение за справяне с него – **не е препоръчителен**. Вместо това организациите **следва да предвидят и установят** ясни процедури за действие в такива ситуации. Неспазването на това изискване **може да подкопае доверието** във вътрешния канал за подаване на сигнали, тъй като могат да възникнат опасения относно пристрастност или липса на обективност, което да доведе до загуба на доверие в администрирането на сигналите.

Призната **добра практика** е да се изисква от лицата, отговарящи за разследванията, да попълнят декларация за липса на конфликт на интереси преди да вземат участие във вътрешна процедура по сигнализиране. Това помага да се гарантира, че назначеният персонал няма лични или професионални връзки, които биха могли да повлияят на безпристрастността му.

Разследванията са **ограничени във времето**. Те трябва да продължат колкото е необходимо, но не могат да надвишават период от три месеца, освен в случаите с особена сложност, при които производството може да бъде удължено с още три месеца. Решението за удължаване с още три месеца следва да бъде взето преди изтичането на първоначалния срок, като се посочат причините, които са попречили на своевременното приключване на разследването, и се обоснове причината, довела до необходимостта от удължаване.

2.5.3 Съображения за защита на данните

Член 17 от Директивата определя, че всяко **обработване на лични данни**, извършено в процеса на нейното прилагане, трябва да е в съответствие с Регламент (ЕС) 2016/679 и Директива (ЕС) 2016/680. Освен това **всеки обмен или предаване на данни** от институциите, органите, службите или агенциите на ЕС трябва да се извършва в съответствие с Регламент (ЕС) 2018/1725, който урежда защитата на данните в институциите на ЕС.

Тук се включва и принципа на минимизиране на данните, който има за цел да предотврати събирането на данни, които не са необходими за разследването на сигнала. Ако случайно бъдат събрани такива данни, те трябва да бъдат изтрети незабавно.

От съществено значение е, обаче, да се вземе предвид и националното законодателство по отношение на специфични аспекти като достъпа до лични данни, съдържащи се във вътрешния канал, регистъра на сигналите и преписките, както и периодите на съхранение на данните, установени от националното законодателство.

Съгласно съображение 83 от Директивата следва да се обърне специално внимание на основните принципи, свързани с

обработването на лични данни, установени в член 5 от Регламент (ЕС) 2016/679, член 4 от Директива (ЕС) 2016/680 и член 4 от Регламент (ЕС) 2018/1725, както и на принципа на защита на данните още при проектирането и по подразбиране, уреден в член 25 от Регламент (ЕС) 2016/679, член 20 от Директива (ЕС) 2016/680 и членове 27 и 85 от Регламент (ЕС) 2018/1725.

Важно е да се припомни съдържанието на член 5 от Регламент (ЕС) 2016/679⁵³, в който се посочва, че **ръководните принципи за гарантиране** на легитимността на обработването на лични данни са принципът на проактивна отговорност, принципът на законосъобразност, добросъвестност и прозрачност, принципът на ограничаване на целите, принципът на свеждане на данните до минимум, принципът на точност, принципът на ограничение на съхранението и принципът на цялостност и поверителност. **(За повече подробности, вижте Глава 3).**

Гл.3 >

2.6 ПРОЦЕС НА РАЗСЛЕДВАНЕ В РАМКИТЕ НА ВЪТРЕШНАТА СИСТЕМА ЗА СИГНАЛИЗИРАНЕ

Препоръчително е да се създаде система за идентифициране на сигнали, заедно със запис на получената информация и проведените вътрешни разследвания. Специално внимание трябва да се обърне на ограничаването на сроковете за съхранение на лични данни, **за повече информация вижте Глава 3**. По време на фазата на получаване на сигнала лицето, сигнализиращо за нередности, трябва да получи **потвърждение за получаване в рамките на седем дни**. Това потвърждение е от съществено значение, тъй като служи като доказателство, че лицето, сигнализиращо за нередности, е подало сигнал чрез **вътрешния канал за подаване на сигнали**. То може да се изисква и при искане на мерки за защита и/или подкрепа от компетентния орган.

След като бъде получен сигнал, следващият етап от процедурата за вътрешно разследване може да бъде преценката за **допустимост на сигнала**. Лицето, отговарящо за вътрешния канал, трябва да оцени

⁵³ Член 5. Принципи, свързани с обработването на лични данни

1. Личните данни са:

а) обработвани законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните („законосъобразност, добросъвестност и прозрачност“);
б) събирани за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели; по-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита, съгласно член 89, параграф 1, за несъвместимо с първоначалните цели („ограничение на целите“);
в) подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“);
г) точни и при необходимост да бъдат поддържани в актуален вид; трябва да се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват („точност“);
д) съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни; личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели съгласно член 89, параграф 1, при условие че бъдат приложени подходящите технически и организационни мерки, предвидени в настоящия регламент с цел да бъдат гарантирани правата и свободите на субекта на данните („ограничение на съхранението“);
е) обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност“);
2. Администраторът носи отговорност и е в състояние да докаже спазването на параграф 1 („отчетност“).

сигнала и да вземе обосновано решение за една от следните възможности:

- недопустимост на сигнала;
- допускане на сигнала за обработка;
- препращане на сигнала на прокуратурата, Европейската прокуратура или друг компетентен орган.

Примери за критерии за недопустимост

Сигналът може да се счита за недопустим при следните обстоятелства:

- неразбираеми, неправдоподобни твърдения, включително очевидно неверни твърдения без обективна основа;
- липса на минимално описание на фактите, като например времето, мястото или естеството на предполагаемото нарушение или нередност;
- позоваване единствено на слухове, спекулации или предположения;
- позоваване на същите факти, по които вече е имало разследване и решение от организацията, освен ако не са предоставени нови доказателства или съществена информация.

Що се отнася до първото основание за недопустимост, очевидно неверни твърдения, съображение 101 предвижда запазване на защитата, когато съобщените факти са неточни или подвеждащи, съгласно правилата на общото национално право. Член 23 от Директивата, обаче, изисква от държавите членки да налагат санкции за съзнателно подаване на неверни или злонамерени сигнали, за да се предотвратят нови неверни или злонамерени сигнали и да се запази надеждността на системата. Тези санкции трябва да бъдат пропорционални, като се гарантира, че не създават възпиращ ефект върху добронамерените лица, подаващи сигнали за нередности. Когато се занимават с фалшиви сигнали, задължените субекти трябва да спазват националните транспониращи закони, уреждащи този въпрос.

Според доклада за прилагането на Директивата, публикуван от Европейската комисия, по отношение на **този режим на санкциониране** в националните транспониращи закони са идентифицирани проблеми, свързани със съответствието, като например:

- липса на правна сигурност за това кое поведение подлежи на санкциониране;
- неефективно ниски глоби, намаляващи възпиращия ефект;
- санкциониране на ответни действия с цел отмъщение, предприети само срещу сигнализиращите лица, вместо разширяване на защитата по отношение на други категории лица, като например помощници (член 4 от Директивата).

Съгласно **италианското законодателство** сигналът може да се счита за **недопустим** в следните случаи:

- когато липсват данни, които представляват съществени елементи на сигналите (напр. сигнализираните факти и администрацията или организацията, в които са установени; администрацията или организацията, където работи сигнализиращото лице, и професионалният му профил; кратко описание на начина на узнаване за сигнализираните факти и т.н.);
- когато сигнализираните нарушения не попадат в материалния обхват, определен от италианското законодателство;
- когато сигнализиращото лице не е сред законно оправомощените да сигнализира;
- когато фактите в сигнала не са свързани с работната среда.

2.6.1 Какво се случва, когато сигналът бъде допуснат за обработка?

Съдържанието на сигнала се подлага на **проверка за правдоподобност**: всичко, което **не съдържа признаци или елементи на невярна информация**, може да бъде определено като правдоподобно. Сигналът се счита за **правдоподобен**, когато има **достатъчно индикации, които да оправдаят по-нататъшно разследване**. Извършването на задълбочена оценка на правдоподобността е от решаващо значение за избягване на произволни или ненужни разследвания. Правдоподобността на даден сигнал трябва непрекъснато да се преоценява по време на целия етап на разследването, като се гарантира, че събраните доказателства съответстват на сигнализираните факти. След това лицето, за което се твърди, че е отговорно за нарушението, се идентифицира и се събират доказателства.

Това е и моментът, в който трябва да се **предприемат временни мерки, за да се гарантира ефективността** на разследването и да се избегнат щети, които могат да бъдат непоправими на по-късен етап. Тези временни мерки трябва да бъдат планирани във вътрешното производство, надлежно мотивирани и основани на извършен предварителен анализ на необходимостта и пропорционалността им.

2.7 ПРАВОМОЩИЯ ЗА РАЗСЛЕДВАНЕ

Основната цел на вътрешното разследване е да се съберат и запазят доказателствата, необходими за установяване на фактите и определяне на възможните отговорности. **Вътрешните разследвания** нямат същия обхват или **правно естество** като съдебните разследвания, тъй като са от административен характер. Всяко събиране на доказателства **трябва стриктно да избягва** използването на незаконни, несправедливи или неетични методи, които нарушават основните **права и свободи**, както

индивидуални, така и колективни⁵⁴. Разследване, при което не се спазват тези граници при събирането на доказателства, може да доведе до **сериозни последици**, включително обезсилване на събраните доказателства и **потенциална наказателна отговорност** за лицата, които провеждат разследването. По принцип вътрешните разследвания разчитат на **различни средства за проверка**, като най-често срещаните са:

- документация и/или информация, която съдържа данни и доказателства, и;
- персонални интервюта.

За да проверят точността на сигнализираните факти, разследващите лица обикновено изискват **документи и доклади**, съдържащи необходимите данни като доказателства.

Тези източници на данни могат да бъдат категоризирани като:

- **вътрешни източници:** различни организационни звена трябва да сътрудничат на разследването, тъй като те могат да притежават ценни документи, които изясняват обстоятелствата по случая;
- **общодостъпни източници:** сред многото, които могат да бъдат проверени, се предлагат някои основни като:
 - данни за обществени поръчки и други поръчки могат да бъдат получени чрез справка в регистри и платформи с данни за обществените поръчки и на порталите за отворени данни на субектите от публичния сектор;
 - търговски данни могат да бъдат получени от публични търговски регистри и официални бюлетини;
 - данни от администрации и институции от публичния сектор, като общи данни, бюджети, годишни отчети, лица, заемащи изборна длъжност, лица на ръководни позиции и други служители, организационни схеми и други могат да бъдат намерени на порталите за прозрачност и отворени данни на съответните организации;
 - данни за безвъзмездно отпуснати средства и субсидии могат да бъдат получени от регистри за субсидии, портали за отворени данни на различни субекти, както и в официални бюлетини;
 - данни от избирателните списъци също могат да бъдат получени от общодостъпни източници;
 - данни от регистри на заинтересовани групи или други подобни;
 - данни от програмите на високопоставени служители.

Когато се използват общодостъпни източници, от решаващо значение е да се **оцени надеждността на информацията**. Такива данни често трябва да бъдат филтрирани, валидирани и подложени на кръстосана проверка, за да се гарантира тяхната точност. **Добра практика за запазване на поверителността е тази документация да не се изисква**

⁵⁴ Относно признаването на личния живот в контекста на работата е препоръчително е да се направи справка с решението на ЕСПЧ по делото *Bărbulescu v. Romania (Bărbulescu II)* от 5 септември 2017 г.

от отделите или звената на самата организация, ако може да бъде получена чрез справка в общодостъпни източници.

2.7.1. Какви са препоръките за персонално интервю?

- Провеждане на интервютата в присъствието на поне двама разследващи служители.
- Предвиждане на условията за преценка при провеждане на интервюто и начина, по който интервюто трябва да бъде документирано и записано, както и предоставяне на необходимата информация относно обработването на личните данни на интервюираните лица съгласно разпоредбите на Общия регламент относно защитата на данните (чл. 15 и следващите).
- Първото лице, което трябва да бъде интервюирано, трябва да бъде сигнализиращото лице (ако сигналът не е подаден анонимно). След това интервютата трябва да продължат с хора, които може да имат информация или да са били свидетели на сигнализираните факти или поведение, и накрая остават възможните участници и/или лицата, отговорни за фактите.
- Трябва да се определи дали интервюираният може да бъде придружен от адвокат или друго лице (помощник, представител на синдикат и т.н.).

2.7.2. Приключване на вътрешното разследване

Вътрешното разследване трябва да бъде прекратено, когато се установи, че е неоснователно или необосновано.

Ако сигнализираните факти се потвърдят, възможните начини за **приключване** на вътрешното разследване са следните:

- **информирание на компетентния отдел** или звено, за да може да бъдат предприети мерки за разрешаване на сигнализираното нарушение, включително налагане на дисциплинарни мерки;
- **препращане на компетентен административен орган** при потвърждаване на нарушението;
- **препращане на прокуратурата** и/или друг съдебен орган, когато сигнализираните факти съставляват престъпление; ако предполагаемото действие засяга финансовите интереси на Европейския съюз, сигналът следва да бъде препратен на Европейската прокуратура;
- вътрешни препоръки в случай на установени лоши практики и липса на професионализъм.

2.7.3. От вътрешно разследване до прокуратурата

Задължението за **изпращане на информация** от вътрешно разследване на **прокуратурата или съдебните органи** е включено при транспонирането на Директивата от страна на **Испания**. Тази разпоредба обаче е **противоречива**, особено за **юридическите лица, подлежащи на корпоративна наказателна отговорност**. В някои случаи задължителното подаване на сигнали може да влезе в конфликт с правото на юридическите лица да не се самоуличават в престъпление. Това може да усложни някои разследвания и да повдигне правни въпроси. **Процедурата за администриране на сигналите** трябва да предвижда възможност за издаване на **препоръки** за определяне на начина, по който тези ситуации трябва да бъдат третирани, и за включването им в процесите на непрекъснато подобряване на организацията. В противен случай системата за вътрешно сигнализиране ще загуби смисъла си на система, първоначално замислена като възможност за укрепване на институционалната почтеност и етичната култура в организацията.

Препоръките, произтичащи от вътрешно разследване, могат да служат за различни цели, като например:

- разработване на програми за обучение или повишаване на осведомеността;
- подобряване на вътрешните процеси или протоколи;
- гарантиране на правилното прилагане на коригиращи мерки;
- информиране на органа за контрол съответствието относно спазването на етичния кодекс или кодекса за поведение, и др.

Както **лицето, засегнато от сигнала**, така и **сигнализиращото лице** трябва да бъдат **информирани за резултата от разследването**. Директивата признава правото на сигнализиращото лице да получава актуална информация за движението на своя сигнал и да бъде уведомено за окончателните резултати от разследването.

Препоръчително е **докладът или документът, с който приключва разследването**, да включва информация за начина на започване на разследването, предмета на разследването, **извършените действия**, участващите лица, оценката на достоверността на фактите, както и заключенията и предложенията, с които **завършват последващите действия** по сигнала и, както се **посочва в Директивата**, се разрешава сигнализираното нарушение. Във всеки случай тази информация трябва да бъде обективна, безпристрастна, ясна и точна.

2.8. РОЛЯ НА ВЪНШНИЯ КАНАЛ ЗА СИГНАЛИЗИРАНЕ

2.8.1. Значение на ефективните канали за подаване на сигнали за нередности

Съгласно **съображение 63** от Директивата **липсата на доверие в ефективността на каналите за подаване на сигнали** е един от основните фактори, които възпират лицата, които биха сигнализирали за нередности. За да се справят с този проблем, от компетентните органи се изисква да създадат независими и автономни външни канали за подаване на сигнали, които да гарантират **надлежно проследяване** на получените сигнали и да предоставят навременни отговори на лицата, подаващи сигнали за нередности. В случаите, когато вътрешните канали не съществуват, не функционират правилно или когато **лицата, сигнализиращи за нередности, се страхуват от ответни мерки**, компетентните органи може да са по-подходящи от самите организации за обработка на сигналите и последващи действия във връзка с тях. **Член 11** от Директивата предвижда, че тези външни канали за подаване на сигнали трябва да бъдат както независими, така и автономни при получаването и обработването на сигнали за нарушения. Освен това **съображение 65 подчертава**, че компетентните органи трябва да разполагат с необходимия капацитет и правомощия за извършване на подходящи последващи действия, оценка на точността на сигналите, справяне с нарушенията чрез разследване или наказателно преследване и предприемане на корективни мерки, ако е необходимо. При необходимост **органите трябва** също така да могат да отнасят случаите до **друг компетентен орган**, за да осигурят предприемането на подходящи последващи действия.

2.8.2. Предизвикателства при прилагането и роля на компетентните органи

Прилагането на директивата **среща предизвикателства**, като някои държави членки не са определили окончателно компетентни органи. Освен това около половината от държавите членки са **транспонирали неправилно член 11, параграф 6**, който очертава задълженията на органите, които получават сигнали, но нямат правомощия да ги разгледат. Например някои държави вменяват тези задължения **само на конкретни органи**, без да гарантират сигурното и навременно препращане на сигналите или като пропускат изискването за информиране на сигнализиращото лице.

Когато външните канали за сигнализиране са централизирани, държавите членки трябва да гарантират спазването на изискванията на Директивата за **независимост и автономност**. Членове 12 и 18 от Директивата установяват строги критерии за външните канали за подаване на сигнали, включително гарантиране на целостта и **поверителността на информацията**, дългосрочното съхранение и

достъпността както за писмени, така и за устни сигнали, включително анонимни сигнали, когато такива са разрешени от националното законодателство. **Член 13** изисква от компетентните органи да публикуват ясна и достъпна информация относно процедурите за подаване на сигнали, обжалването, **защитата срещу ответни действия с цел отмъщение** и поверителните съвети за лицата, сигнализиращи за нередности. Освен това **трябва да се извършват периодични прегледи** на всеки три години, за да се гарантира, че процедурите за сигнализиране остават ефективни. Компетентните органи не само администрират **външни канали**, но също така могат да **налагат санкции** и да играят жизненоважна роля в изграждането на култура, която насърчава подаването на сигнали за нередности, като гарантира, че тези, които съобщават за нарушения, не стават жертва на стигматизация или отмъщение.

2.8.3. Едновременно сигнализиране по вътрешни и външни канали

Въпреки че Директивата не изисква лицата, сигнализиращи за нередности, да подават сигнали вътрешно, преди да използват външни канали, тя не разглежда изрично как да се обработват едновременно вътрешни и външни сигнали. Този въпрос беше обсъден на четвъртото **заседание на експертната група**, на което бяха отправени препоръки към държавите членки да включат разпоредби в своите транспониращи закони:

- Лицата, подаващи сигнали за нередности, трябва да изчакат изтичането на тримесечния срок, преди да подадат сигнал по външен канал.
- Ако изберат да сигнализират по външен канал преди изтичане на тримесечния срок, те следва да оттеглят вътрешния си сигнала, подаден по вътрешния канал.

Освен това националните закони биха могли да позволят на съответните органи да изискват съгласие от лицата, подаващи сигнали за нередности, да бъде уведомен техния работодател за подадения сигнал. Въпреки това, лицата, подаващи сигнали, никога няма да загубят защитата си, ако спазят тези препоръки.

Според Европейската комисия на практика външният сигнал би довел до мълчаливо оттегляне на вътрешния сигнал. Ако работодателят узнае за външно разследване, вътрешният канал вече няма да бъде задължен да проследява сигнала. Въпреки това организацията може да избере да продължи вътрешното си разследване. Ако вътрешното и външното разследване продължават едновременно, компетентните органи остават задължени да разследват и да предприемат мерки за отстраняване на нарушенията съгласно Директивата.

Във всеки случай транспониращото законодателство следва да уреди начините за справяне със сигнали, подадени едновременно по вътрешния и външния канал, когато сигнализиращото лице е подало сигнал по външния канал преди изтичането на тримесечния срок за вътрешното разследване, в съответствие с препоръките, отправени от експертната група.

2.9. ПРЕПОРЪКИ

1. СПАЗВАНЕ НА КОНФИДЕНЦИАЛНОСТТА

Трябва да се прилагат процедурни, технически, организационни мерки и мерки за сигурност, за да се запази поверителността на личните данни, съдържащи се във вътрешните канали за подаване на сигнали. Специален акцент трябва да се постави върху гарантирането и запазването на поверителността както на лицето, подало сигнал, така и на лицата, засегнати от сигнала. Вътрешните разследвания също трябва да се провеждат по начин, който минимизира риска от нарушаване на поверителността по време на целия процес.

2. ПРОЦЕДУРИ ЗА МОНИТОРИНГ

Процедурите за администриране и наблюдение на вътрешните сигнали трябва да бъдат подробни и да съдържат, в допълнение към минималното съдържание и принципи, предвидени в транспониращото законодателство, възможно най-подробно описание на различните етапи на процедурата за проследяване на сигналите и на действията, които трябва да се извършат във всеки от тях. Те следва също така да посочват какви ще бъдат използваните средствата за проверка.

3. ИДЕНТИФИКАЦИЯ НА СИГНАЛА

Трябва да има система за идентифициране на сигналите, както и регистър на получените сигнали и проведените разследвания. Това гарантира проследимост на действията на вътрешния канал и подобрява отчетността.

4. ОПРЕДЕЛЯНЕ НА ДОПУСТИМОСТТА

Процедурата за администриране на сигналите трябва да определя обстоятелствата, при които даден сигнал ще се счита за недопустим.

5. ПЛАНИРАНИ ВЪТРЕШНИ РАЗСЛЕДВАНИЯ

Вътрешните разследвания трябва да бъдат правилно планирани, с ясен график, за да се предотвратят неоправдани забавяния, които биха могли да надхвърлят определения срок. Планът следва да определя:

- обхвата на разследването;
- източниците на доказателства и необходимата документация;
- участващите лица и тези, които трябва да бъдат интервюирани;

6. ГРАНИЦИ НА ДОКАЗАТЕЛСТВОТА

Събирането на доказателства при вътрешни разследвания трябва да се извършва при спазване на ограниченията за събиране на доказателства, като във всеки случай се зачитат основните права и принципи, признати в Хартата на основните права на ЕС, както и разпоредбите на националното законодателство и вътрешните процедури и протоколи, одобрени от организацията.

7. МИНИМИЗИРАНЕ НА ИСКАНИЯ ЗА ДОКУМЕНТИ И НАПОМНЯНЕ ЗА ПОВЕРИТЕЛНОСТ

Не трябва да се изисква документация от отделите в организацията, ако тези данни могат да бъдат получени от общодостъпни източници (например, информация за назначаването на държавен служител, публикувана в Държавен вестник), а на интервюираните лица и на отделите, от които се налага да се поиска информация и/или документация, трябва да се напомнят задълженията за поверителност и последиците, до които може да доведе тяхното нарушаване.

8. ОБОСНОВКА НА СЪБИРАНЕТО НА ДОКАЗАТЕЛСТВА В ДОКЛАДИТЕ

Докладите от разследваният трябва да включват обосновка на предприетите действия и методите за проверка, използвани при събиране на доказателствата.

9. ПЛАНИРАНЕ И ДОКУМЕНТИРАНЕ НА ИНТЕРВЮТА

На етапа на планиране на разследването е необходимо да се определят критериите за вземане на решение кои лица следва да бъдат интервюирани и в какъв ред, както и да се предвидят условията за преценка за това и как тези действия следва да бъде документирани и записани. Препоръчително е интервютата да се извършват от двама разследващи служители.

10. СТРУКТУРА НА ОКОНЧАТЕЛНИЯ ДОКЛАД ЗА РАЗСЛЕДВАНЕТО

Докладите, с които приключват разследванията, трябва да включват: как е започнало разследването, целите на разследването, предприетите действия и участващите лица, оценка на точността на фактите и заключения и препоръки за разрешаване на сигнализираното нарушение.

11. ОСИГУРЯВАНЕ НА ОБЕКТИВНОСТ И ЯСНОТА В ОТЧЕТИТЕ

Окончателният доклад трябва да бъде обективен, безпристрастен, ясен и точен.

12. УПРАВЛЕНИЕ НА КОНФЛИКТИ НА ИНТЕРЕСИ ПРИ ПОСЛЕДВАЩИ ДЕЙСТВИЯ

Процедурата за последващи действия трябва да включва механизми за идентифициране, управление и предотвратяване на конфликтите на интереси сред лицата, отговорни за разглеждането на сигналите.

13. ПРЕПОРЪКИ ЗА ОРГАНИЗАЦИОННО ПОДОБРЕНИЕ

Процедурата за администриране на сигналите трябва да дава възможност за издаване на препоръки за преодоляване на установените лоши практики и липса на професионализъм (нередности), които да бъдат включени в процесите на непрекъснато подобряване на организацията.

14. УДЪЛЖАВАНЕ НА СРОКОВЕТЕ ЗА ПРОУЧВАНЕ

Ако разследването не може да приключи в рамките на първоначалния тримесечен период, той може да бъде удължен с още три месеца. Това удължаване, обаче, трябва да бъде одобрено преди изтичането на първоначалния срок, да се обоснове причината за забавянето и да се посочат висящите действия, които трябва да бъдат завършени.

15. НАСЪРЧАВАНЕ НА КУЛТУРА НА ПОДАВАНЕ НА СЪОБЩЕНИЯ

Компетентните органи трябва да насърчават култура на подаване на сигнали.

16. РАБОТА С РАННО ВЪНШНО СИГНАЛИЗИРАНЕ

Транспониращото законодателство трябва да уреди как се процедира в случаите, когато лицето е подало сигнал по външен канал преди да е изтекъл тримесечният период на вътрешното разследване. Това трябва да бъде в съответствие с препоръките на експертната група на Европейската комисия.

17. САНКЦИИ ЗА НАРУШЕНИЯ НА ПОВЕРИТЕЛНОСТТА

Необходими са **възпиращи и ефективни санкции за неспазване на изискването за поверителност**, които конкретно се отнасят до нарушението на тази разпоредба от Директивата. Поради това в случай на нарушение на поверителността и задължението за конфиденциалност е необходимо да се обърне внимание на видовете нарушения, предвидени в националното законодателство за транспониране на Директивата. В случая с испанския транспониращ закон⁵⁵, например, като тежки или много тежки са квалифицирани следните нарушения:

- нарушение на гаранциите за поверителност и анонимност, предвидени в закона, и по-специално всяко действие или бездействие, което има за цел да разкрие самоличността на сигнализиращото лице, когато то е избрало да остане анонимно, дори ако самото разкриване не е настъпило;
- нарушение на задължението за запазване на тайна по всеки аспект, свързан със сигнала; споменаването на това правило при обучението на персонала по отношение на поверителността е от значение, тъй като нарушаването на задължението за конфиденциалност, поверителност и анонимност може да представлява, както вече беше споменато, специфично нарушение.

⁵⁵ Закон № 2/2023 от 20 февруари 2023 г., уреждащ защитата на лицата, които съобщават за нарушения на нормативната уредба, и борбата с корупцията.



Защита на личните данни



Глава 3

ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

ГЛАВА 3

3.1 РОЛЯТА НА ЗАЩИТАТА НА ДАННИТЕ В СИСТЕМИТЕ ЗА ПОДАВАНЕ НА СИГНАЛИ

В зависимост от **вида на сигнала**, част от **процеса на подаване на сигнали** може да включва събирането, използването и разкриването на **лични данни**, като ги поставя в пресечната точка на рамките за защита на данните и защита на лицата, сигнализиращи за нередности. Гарантирането на спазването на принципите за защита на данните, като същевременно се гарантира поверителността и правата на сигнализиращите лица, е от съществено значение за поддържане на доверието и спазването на законовите изисквания. Защитата на данните не е просто регулаторно задължение – **тя е инструмент, предназначен да подкрепя**, обслужва и отговаря на нуждите на всички страни, участващи в процеса на подаване на сигнали. Стабилните рамки за защита на данните далеч не са пречка за организационните работни процеси, **а осигуряват яснота и структура**, като гарантират, че лицата, подаващи сигнали, се чувстват уверени при съобщаването на неправомерно поведение и търсенето на помощ от службите за подкрепа, като същевременно защитават интересите на организациите, които получават и обработват такива сигнали. Когато се прилагат внимателно, **мерките за защита на данните могат да насърчат** култура на доверие, да повишат прозрачността и да гарантират целостта на вътрешните системи за сигнализиране.

Общият регламент относно защитата на данните (GDPR), като крайъгълен камък на защитата на данните в Европейския съюз, установява правната рамка за обработване на лични данни и балансиране на правата и задълженията на всички заинтересовани страни (вижте **Глава 1** за разликата между анонимност и поверителност). Специфичните предизвикателства при обработването на чувствителни и лични данни в контекста на подаване на сигнали за нередности подчертават значението на привеждането на стратегиите за защита на данните в съответствие с изискванията на Директивата относно защитата на лицата, сигнализиращи за нередности. На национално равнище рамките за защита на данните в системите за подаване на сигнали изискват щателно планиране и стратегическо привеждане в съответствие с националния правен и културен контекст.

Организацията на обединените нации (ООН) подчертава важността на защитата на лицата, подаващи сигнали за нередности, от ответни мерки като крайъгълен камък на прозрачността и отчетността⁵⁶. Механизмите за подаване на сигнали трябва да дават приоритет на поверителността на хората, за да предотвратят всякаква форма на репресии. Това включва проектиране на сигурни канали за сигнализиране, осигуряване на анонимност и приемане на технологии като криптиране за защита на чувствителните данни. **Политиката на ООН „Защита срещу отмъщение“** илюстрира критичната роля на сигурността на данните в насърчаването на култура, в която хората се чувстват сигурни да съобщават за нарушения, без да се страхуват от лична или професионална вреда.

3.2 ОСНОВНА КОНЦЕПЦИЯ И ОСНОВНИ ПРИНЦИПИ ЗА ЗАЩИТА НА ДАННИТЕ

Взаимодействието между **Общия регламент относно защитата на данните** и **Директива 2019/1937/ЕС относно лицата, сигнализиращи за нередности**, създава правната рамка, за да се гарантира, че личните данни се обработват законосъобразно, етично и прозрачно. Когато **принципите за защита на данните** са включени в разработването на механизмите за подаване на сигнали за нередности, те повишават тяхната надеждност и гарантират спазването както на **правните**, така и на **етичните** стандарти.

3.2.1 Защо защитата на данните е от съществено значение за защитата на лицата, сигнализиращи за нередности?

- **Защита на лична**, чувствителна и поверителна информация от злоупотреба, кражба, неоторизиран достъп и др.
- **Запазва неприкосновеността на личния живот**, като осигурява контрол върху личните данни, намалявайки риска от увреждане или експлоатация.
- **Предотвратяването на кражба на самоличност** и измами е ключово предимство, тъй като нарушенията, разкриващи чувствителна информация, могат да имат опустошителни последици. Бизнесът също печели доверие, като дава приоритет на защитата на данните, което укрепва отношенията с клиентите и партньорите за защита на данните, тъй като неспазването може да доведе до сериозни глоби и щети на репутацията.

Освен тези практически ползи, **защитата на данните е етична отговорност**, която насърчава справедливостта и прозрачността посредством начина, по който се обработва информацията. В един взаимосвързан свят стабилната сигурност на данните също така смекчава заплахите за киберсигурността, като дава приоритет на защитата на данните, а хората и организациите създават по-безопасна и по-надеждна среда.

⁵⁶ Protection against Retaliation [Защита срещу отмъщение] - <https://www.un.org/en/ethics/protection-against-retaliation/index.shtml#:~:text=The%20UN's%20protection%20against%20retaliation,by%20any%20person%20that%20is>

3.2.2 Основни принципи за защита на данните

Принципът на законосъобразност, добросъвестност и прозрачност изисква обработката на данни да се придържа към правните стандарти и да се извършва прозрачно, за да се поддържа доверието. Организациите следва ясно да съобщават целите на събирането на данни на субектите на данни, като гарантират, че техните права са разбрани и зачитани. Накратко, принципите, залегнали в член 5 от GDPR⁵⁷, са отправна точка за гарантиране на спазването на правилата за защита на данните и гарантиране на справедлива, прозрачна и сигурна среда за операциите по обработване на данни:

- Принципът на **законосъобразност, добросъвестност и прозрачност** подчертава значението на обработването на лични данни по начин, който е в съответствие със закона и зачита правата на засегнатите лица. В контекста на подаването на сигнали за нередности законосъобразността задължава организациите да осигурят правно основание за обработването на данните, като например спазване на правно задължение или преследване на законни интереси, като например разследване на неправомерно поведение. Данните следва също така да се обработват по справедлив начин, като се осигури прозрачност, което ще изисква от организациите да информират лицата, сигнализиращи за нередности, за това как техните данни ще бъдат събирани, използвани, съхранявани и потенциално споделяни, като се гарантира, че разбират последиците от тяхното разкриване.
- Принципът за **ограничение на целите** предвижда, че личните данни, събрани чрез каналите за подаване на сигнали, трябва да се използват само за конкретните цели, за които са събрани. Например, ако лице, сигнализиращо за нередности, съобщи за твърдения за измама, предоставената информация трябва да се използва стриктно за разследване на сигнализирания проблем, а не за други цели, като например оценка на работата на лицето, сигнализиращо за нередности. Този принцип защитава от злоупотреба с данни и гарантира, че правата на лицата, подаващи сигнали за нередности, и на другите замесени лица не са несправедливо компрометирани.
- **Минимизирането на данните** е ключов принцип, който подчертава необходимостта от събиране само на данните, които са строго необходими за разследването на сигнализирания въпрос. Прекомерното събиране на данни не само увеличава риска от нарушения или злоупотреба, но също така може да намали доверието на лицата, подаващи сигнали, в поверителността на процеса на подаване на сигнали. Например подробности за трети страни или самоличността на сигнализиращото лице следва да се разкриват само когато са абсолютно необходими за разследването и в съответствие с приложимите закони.
- Принципът на **точност** гарантира, че всички лични данни, обработвани в контекста на подаване на сигнали, са верни и актуални. Неточните данни могат да доведат до несправедливи резултати, като неоснователни обвинения или неправилно приключване на разследванията. Организациите трябва да

⁵⁷ Общ регламент относно защита на данните – <https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:32016R0679>

прилагат процедури за проверка на точността на информацията, предоставена от сигнализиращите лица, и за своевременно отстраняване на неточностите, ако бъдат установени.

- **Ограничението на съхранението** изисква личните данни да се съхраняват само толкова дълго, колкото е необходимо за изпълнение на целта, за която са събрани. В случаите на подаване на сигнали за нередности това означава, че данните следва да се съхраняват само по време на разследването и всяко последващо съдебно или административно производство. Запазването на данни за неопределено време може да изложи физическите лица на неоправдани рискове, като нарушения или злоупотреба, и би било в противоречие с установените принципи за защита на данните.
- Принципите на **цялостност и поверителност** съгласно GDPR са от първостепенно значение, например когато в случая на лицата, подаващи сигнали за нередности, може да бъде предоставена изключително чувствителна информация, и е отговорност на организациите да гарантират, че тези данни са защитени. Строгите мерки като криптиране, контрол на достъпа и сигурни канали за подаване на сигнали са от съществено значение за предотвратяване на неоторизиран достъп, нарушения на сигурността на данните и други рискове, които биха могли да застрашат поверителността на лицата, подаващи сигнали за нередности, или почтеността на разследванията.
- Принципът на **отчетност** изисква организациите да демонстрират спазването на законите за защита на данните при разглеждането на случаи на подаване на сигнали. Това включва поддържане на регистър на дейностите по обработване на данни, извършване на оценки на въздействието върху защитата на данните за системите за подаване на сигнали за нередности и гарантиране, че всички трети страни, участващи в разследването, като например външни одитори или разследващи, се придържат към съответните разпоредби за защита на данните. В Регламент (ЕС) 2016/679 са взети предвид изискванията за поверителност, определени в други правни актове както на национално равнище, така и на равнището на ЕС, и се предвижда да се отчитат само видът данни, а не самите данни.

В допълнение към тези основни принципи защитата на лицата, сигнализиращи за нередности, трябва да разглежда и специфични съображения като анонимността, балансирането на правата между сигнализиращите лица и замесените страни, както и трансграничното предаване на данни. Предоставянето на анонимни канали за подаване на сигнали е в съответствие с целта за защита на сигнализиращите лица от ответни мерки. В същото време организациите трябва да балансират поверителността на сигнализиращите лица с правата на замесените лица на достъп до информация относно твърдения, отправени срещу тях, като гарантират, че това се прави в съответствие със законовите изисквания. Когато подаването на сигнали за нередности включва международни въпроси, организациите трябва да гарантират, че всяко трансгранично предаване на данни е в съответствие с приложимите разпоредби, като например Общия регламент относно защитата на данните в ЕС. От решаващо значение е организациите да се придържат

към тези принципи, така че да могат да защитават правата на всички участващи страни, да гарантират спазването на правните рамки и да насърчават култура на отчетност и прозрачност в системите за защита на лицата, подаващи сигнали за нередности, и да спомагат за култивирането на доверие.

3.3 ПРАВНО ОСНОВАНИЕ ЗА ЗАКОНОСЪОБРАЗНО ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Член 6 от GDPR

Организациите, участващи в процесите по подаване на сигнали за нередности, трябва да идентифицират правно основание за обработване на лични данни, както е посочено в член 6 от GDPR⁵⁸. Правните основания за обработване включват съгласие, договорна необходимост, правно задължение, жизненоважни интереси, обществен интерес и законни интереси:

- **Съгласие**, обработването на лични данни е законосъобразно, когато субектът на данните свободно е дал конкретно, информирано и недвусмислено съгласие данните му да бъдат обработвани за определена цел. Съгласието трябва да бъде ясно, изрично (ако се обработват чувствителни данни) и лесно оттеглимо по всяко време.
- **Основанието за договорни отношения** се прилага, когато обработването се изисква за изпълнение на договор, по който субектът на данните е страна, или за предприемане на преддоговорни стъпки по искане на субекта на данните. Това гарантира, че обработването на данни е пряко свързано с изпълнението или подготовката на договорно задължение (защитата на лицата, подаващи сигнали за нередности, може да бъде част от разпоредбите на всеки договор).
- **Правното задължение** е законосъобразно, когато е необходимо да се спази конкретно законово изискване, наложено на администратора на данни. Това основание обикновено се използва, когато законодателството задължава запазването, докладването или споделянето на данни (съгласно законодателни актове, като Директивата и националното законодателство, защитата на лицата, сигнализиращи за нередности, е предмет на правни задължения, приложими за организациите).
- **Жизненоважни интереси е основание, което** оправдава обработването, когато е необходимо да се защити животът или физическата безопасност на субекта на данните или на друго лице. На това основание често се разчита при спешни случаи, като медицински ситуации, където не може да се получи съгласие.
- **Общественият интерес или упражняването на официални правомощия** се прилага, когато обработването е необходимо за изпълнение на задача от обществен интерес или за упражняване на официални правомощия, предоставени на администратора на данни. Това обикновено се използва от публични органи или организации, действащи съгласно закони или подзаконови

⁵⁸ Общ регламент относно защита на данните – <https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:32016R0679>

разпоредби, като същевременно следва да бъде изрично посочено в конкретния правен акт.

- **Легитимни интереси**, означава, че обработването е законосъобразно, когато е необходимо да се постигнат законните интереси на администратора на данни или на трето лице, при условие че тези интереси се прилагат преимуществено пред правата и свободите на субекта на данните. Това основание изисква внимателен тест за балансиране, за да се гарантира, че обработването не засяга несправедливо неприкосновеността на личния живот на субекта на данните (въпреки че изборът на най-подходящото правно основание е в ръцете на организациите, когато е възможно, се препоръчва да се разчита на някое от другите правни основания, предвидени в член 6 от GDPR).

В обобщение, законосъобразното обработване на лични данни съгласно член 6 от GDPR е от съществено значение за гарантиране на спазването и насърчаване на доверието в механизмите за подаване на сигнали за нередности. Организациите трябва внимателно да определят и документират подходящото правно основание, като същевременно балансираат правата на субектите на данни и изискванията съгласно Директивата.

Член 9 от GDPR

Специални категории лични данни, включително информация, свързана с расов или етнически произход, политически възгледи, религиозни убеждения, здраве или сексуална ориентация, подлежат на повишена защита съгласно член 9 от GDPR⁵⁹. Тези видове данни се считат за чувствителни и изискват специфични условия, за да се обоснове обработването им. Изричното съгласие остава основа за обработване на чувствителни данни, но организациите трябва да гарантират, че това съгласие се дава свободно и е добре документирано.

⁵⁹ Общ регламент относно защита на данните – <https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:32016R0679>

РАВЕНСТВО МЕЖДУ ПОЛОВЕТЕ

Чрез интегриране на чувствителни към пола политики в **рамките за защита на данните**, системите за подаване на сигнали за нередности могат да станат по-безопасни и по-ефективни, като насърчават повече хора, особено жени, да се отзовават, без да се страхуват от отмъщение или разобличаване. Тези мерки са от съществено значение, за да се гарантира, че сигналите за неправомерно поведение, основани на пола, се обработват сигурно и самоличността на лицата, подаващи сигнали, остава защитена, особено когато има динамика на властта, която може да повлияе на процеса. Препоръчва се:

- да се наблегне на това как системите за сигурност предотвратяват отмъщението в случаи, основани на пола, като гарантират, че сигналите са защитени от достъп на лица в една и съща йерархия на работното място, като ръководители или колеги, за да се избегне потенциално възмездие;
- да се гарантира, че платформите, които претендират за анонимност, наистина защитават самоличността на лицето, подало сигнал за нередности, особено в случаи, свързани с неравнопоставеност между половете и различните нива на йерархията (напр. работодател-служител, професор-студент, държавен орган-гражданин);
- да се предостави изрична информация за това как мерките за цифрова сигурност (напр. TOR, доказателства с нулево знание, IP маскиране) защитават лицата, подаващи сигнали за нередности, които съобщават за неправомерно поведение, основано на пола;
- да се разработят онлайн платформи и горещи линии за сигнализиране за корупция, предлагащи възможност на физическите лица да разкриват информация от вкъщи, а в някои случаи и анонимно. Този начин на докладване **може да бъде особено удобен за сигнализиране за насилие, основано на пола**, свързано с корупция и сексуално изнудване.

Тези мерки са от съществено значение, за да се гарантира, че сигналите за неправомерно поведение, основани на пола, се обработват сигурно и самоличността на сигнализиращите лица остава защитена, особено когато има динамика на властта, която може да повлияе на процеса.

Протоколи за поверителност за сигнали, основани на пола:

- Определяне на допълнителни мерки за защита на поверителността за лицата, сигнализиращи за нередности, които съобщават за неправомерно поведение, основано на пола, включително мерки за предотвратяване на непрякото идентифициране чрез подробности за случая.
- Подробно описване как сигналите, свързани с насилие, основано на пола, ще бъдат сигурно съхранявани и отделени от общите сигнали за неправомерно поведение, за да се сведе до минимум разкриването.
- Изясняване на това кой има достъп до сигнали и как се прилага защитата на самоличността, като се гарантира, че неупълномощени лица (напр. колеги или преки ръководители) нямат достъп до чувствителни данни.
- Поверителността е от ключово значение за поддържане на целостта на сигнализирането за неправомерно поведение, основано на пола, и за защита на сигнализиращите лица от потенциални вреди.

Други правни основания за обработване на чувствителни данни включват спазване на правни задължения, необходимост от обработване за важен обществен интерес и защита на жизненоважни интереси. Например, случаите на подаване на сигнали за нередности,

включващи твърдения за дискриминация, може да изискват обработването на чувствителни данни за обосноваване на твърдения или спазване на антидискриминационните закони. Организациите трябва да бъдат внимателни и да прилагат допълнителни предпазни мерки при обработването на такива данни, за да намалят рисковете и да гарантират съответствието.

Права на субектите на данни съгласно Регламент (ЕС) 2016/79

GDPR предоставя на субектите на данни набор от права, предназначени да овластят физическите лица и да им осигурят по-голям контрол върху техните лични данни. Сред тях са:

- **Право на достъп**, което позволява на физическите лица да получат подробна информация за обработването на техните данни, включително целите, категориите, получателите и периодите на съхранение.
- **Право на коригиране**, което гарантира, че неточните или непълните данни могат да бъдат коригирани своевременно, повишавайки точността и надеждността на обработваната информация.
- **Правото да се поиска изтриване** на данни при определени обстоятелства, като например когато данните вече не са необходими за първоначалната си цел или когато съгласието е оттеглено. Това право обаче не е абсолютно и трябва да бъде балансирано с необходимостта от запазване на данни за правни или разследващи цели.
- **Право на ограничаване на обработването**, което позволява на физическите лица да ограничат обхвата на дейностите по обработка на данни, особено по време на спорове относно точността или законосъобразността на обработването.
- **Преносимост на данните**, която позволява на хората да получават своите данни в структуриран, често използван и машинно четим формат и да ги прехвърлят на друг администратор. Това право засилва индивидуалната автономност и улеснява конкуренцията между доставчиците на услуги.
- **Право на възразение**, което позволява на физическите лица да оспорват дейности по обработване на данни въз основа на законни интереси или основания от обществен интерес. Организациите трябва внимателно да оценят тези възразения и да предоставят ясни обосновки за продължаване или прекратяване на дейностите по обработване.

Всяка държава определя конкретните процедури за упражняване на правата на субектите на данни съгласно членове 15-22 от GDPR⁶⁰, като това обикновено включва искане до администратора на данни за упражняване на правата им. **Националното законодателство**

⁶⁰ Общ регламент относно защита на данните – <https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32016R0679>

определя дали такива искания следва да се подават по електронен път, в писмена форма или и двете, или чрез специфичен за организацията метод, който не следва да създава допълнителни затруднения за субектите на данни, нито да надвишава непропорционално административната тежест за администратора.

3.4 ВЗАИМОДЕЙСТВИЕ МЕЖДУ ПРАВНАТА РАМКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ И ДИРЕКТИВА 2019/1937/ЕС

Въпреки че GDPR предоставя на субектите на данни спектър от права, винаги трябва да се има предвид взаимодействието му с друго законодателство. **Когато субектите на данни се считат за лица, подаващи сигнали за нередности** съгласно Директивата, **те все още могат да упражняват всяко от правата си съгласно GDPR**, но организациите могат да откажат да изпълнят искания от субектите на данни за упражняване на правата им или директно да откажат, когато това би било в нарушение на правните изисквания за защита на сигнализиращите лица, както съгласно Директивата, така и съгласно националното законодателство. Въпреки че GDPR определя изисквания и срокове, свързани с изтриването на данни, в този случай лицето, което подава сигнала, или просто след приключване на целта, за която са събрани данните, регламентът все още се счита за *lex generalis*. За тази цел, когато в националното законодателство има различни срокове на съхранение за различните видове данни, те се прилагат спрямо тези, определени в GDPR. Освен това, субектите все още могат да използват „**законен интерес**“, но когато го правят, трябва да бъде доказано с достатъчно доказателства.

И двете рамки имат общи цели за насърчаване на прозрачността и отчетността, като същевременно се защитават правата на физическите лица. Поверителното обработване на сигнали за нередности е основно изискване съгласно Директивата и GDPR. И двете рамки предвиждат събирането и обработката само на данните, необходими за постигане на целите на механизма за сигнализиране. Това намалява рисковете, свързани с прекомерното събиране, и гарантира спазването на принципа на ограничаване на целта.

Данните трябва да се съхраняват само толкова дълго, колкото е необходимо за разследване и разрешаване на сигнализираните проблеми. Например, в **Италия** приложимото национално право предвижда, че сигналите не могат да се използват извън необходимото за адекватни последващи действия във връзка с тях. Самоличността на сигнализиращото лице и всяка друга информация, от която тази самоличност може да бъде изведена, пряко или косвено, не могат да бъдат разкривани без изричното му съгласие на лица, различни от компетентните да получават или проследяват сигналите, изрично упълномощени да обработват такива данни съгласно член 29 и член 32,

параграф 4 от Регламент (ЕС) 2016/679⁶¹ (чл. 12.1). Предвижда се също така, че лични данни, които очевидно не са полезни за обработката на конкретен сигнал, не се събират или, ако бъдат събрани случайно, се изтриват незабавно (чл. 13.2). Вътрешните и външните сигнали и свързаната с тях документация се съхраняват за времето, необходимо за обработка на сигнала, и във всеки случай не повече от пет години от датата на съобщаване на окончателния резултат от процедурата за сигнализиране.

Публичните и частните организации определят свой собствен модел за получаване и управление на вътрешни сигнали, като определят технически и организационни мерки, подходящи за гарантиране на ниво на сигурност, адекватно на специфичните рискове, произтичащи от извършеното обработване, въз основа на оценка на въздействието върху защитата на данните. Освен това **италианското законодателство за защита на данните** включва специална разпоредба за защита на поверителността на самоличността на лицето, сигнализиращо за нередности (чл. 2-undecies в Законодателен указ № 196 от 30 юни 2003 г.). Този член е въведен със Законодателен указ № 101 от 10 август 2018 г., за да се съобрази с Регламент (ЕС) 2016/679). Горепосочената разпоредба установява, че в контекста на сигнал засегнатият субект, предполагаем автор на нарушението, по отношение на личните му данни, обработвани от администрацията, не може да упражни правата, предвидени в членове 15-22 от Регламент (ЕС) 2016/679, тъй като упражняването на тези права може да доведе до увреждане на защитата на поверителността на самоличността на сигнализиращото лице. Законът предвижда възможност засегнатото лице да поиска от органа за защита на данните проверки за съответствието на обработването на неговите данни. Органът за защита на данните предоставя обратна връзка относно относителния резултат.

Чрез привеждане на стратегиите за защита на данните в съответствие с изискванията на Директивата за лицата, сигнализиращи за нередности:

- **Организациите** могат да създадат интегрирани системи, които зачитат индивидуалните права, като същевременно подкрепят ефективното управление и съответствие. Лицата, подаващи сигнали, се чувстват уверени, знаейки, че личните им данни ще бъдат третираны с най-голямо внимание.
- **Укрепва се общественото доверие в системите за сигнализиране.**
- **Регулаторите** и организациите трябва да работят съвместно, за да осигурят безпроблемно внедряване, като използват инструменти като стандартизирани протоколи за отчитане, ясни насоки за съхранение на данни и достъпни техники за анонимизиране.

⁶¹ Общ регламент относно защита на данните – <https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32016R0679>

3.5 ЗАЩИТА НА ДАННИТЕ ПРИ ПРОЕКТИРАНЕТО И ПО ПОДРАЗБИРАНЕ ВЪВ ВЪТРЕШНИТЕ КАНАЛИ ЗА ПОДАВАНЕ НА СИГНАЛИ

Организациите могат да изградят стабилни системи за подаване на сигнали, които са в съответствие с принципите за защита на данните по проект и по подразбиране.

3.5.1 Какво представлява защитата на данните още при проектирането?

Вътрешен канал за сигнализиране: вграждане на мерки за сигурност и съображения за поверителност в разработването на механизми за докладване. Например, системите трябва да включват функции като криптирани комуникационни канали, контрол на достъпа, базиран на роли, и одитни регистрационни файлове, за да се гарантира поверителност и отчетност. Минимизирането на данните трябва да ръководи проектирането на формулярите за отчитане и работните потоци, като гарантира, че по време на първоначалния отчет се събира само необходима информация. Организациите следва също така да прилагат процедури за проверка на точността и необходимостта на събраните данни, като същевременно се гарантира анонимността на лицата, сигнализиращи за нередности. Пример за това би било разработването на вътрешни механизми, позволяващи кръстосана проверка на конкретни видове данни, без да се разкрива самоличността на лицето, сигнализиращо за нередности, за да се докаже валидността на твърденията, направени в представените сигнали. Вече съществуват софтуерни решения (включително софтуери, използвани от анализатори на данни), които позволяват на различни бази данни (специфични отдели, човешки ресурси и др.) да проверяват тази информация в анонимен формат.

Казус от Италия: внедряването на софтуерни системи, включващи стабилно криптиране, за да се гарантира поверителност във външните канали за докладване, е еталон за ефективна защита на данните още при проектирането. Пример за това е Globaleaks, който създава идентификатор за всяко сигнализиращо лице, което позволява асинхронна и сигурна комуникация с канала за подаване на сигнали. Подобна практика гарантира, че никоя от страните няма достъп до ненужни лични данни, като по този начин се изпълнява принципът на минимизиране на данните.

3.5.2 Какво представлява защитата на данните по подразбиране?

Организациите следва да обработват само данните, необходими за конкретни цели. Вътрешните системи за сигнализиране трябва автоматично да прилагат най-високите настройки за поверителност и

да ограничават достъпа до данни до определен персонал. Редовните оценки на системните конфигурации и практики гарантират, че тези принципи се прилагат и актуализират последователно за справяне с възникващите рискове и регулаторните промени. За да се засили защитата на данните, организациите следва да приемат иновативни технологии като автоматизирани проверки за съответствие, откриване на аномалии в реално време в потоците от данни и решения за криптирано съхранение (вижте **Глава 1** за допълнителна информация). Ангажирането на служителите чрез семинари или обучения за защита на данните и системите за вътрешно отчитане може да преодолее пропастта между технологията и практическото приложение. Този холистичен подход гарантира, че служителите на всички равнища разбират своите отговорности, като насърчава култура на проактивна защита на данните.

3.6 ЗАЩИТА НА ДАННИТЕ ВЪВ ВЪНШНИТЕ КАНАЛИ ЗА ПОДАВАНЕ НА СИГНАЛИ

Външните канали за подаване на сигнали, като например тези, управлявани от регулаторните органи, са изправени пред допълнителни предизвикателства при балансирането на прозрачността и защитата на данните. **Защитените комуникационни канали** са от съществено значение за защита на целостта на сигналите и предотвратяване на неоторизиран достъп до чувствителна информация. Организациите, работещи с външни канали, следва да установят ясни политики, **очертаващи обработването на личните данни**, включително процедури за проверка на автентичността на сигналите и защита на самоличността на сигнализиращите лица.

Прозрачността е от ключово значение. Лицата, подаващи сигнали за нередности, следва да имат възможности за анонимност и механизми за сигурна последваща комуникация. Защитата, предоставена на лицата, сигнализиращи за нередности, попада в обхвата на законните цели съгласно GDPR, като предоставянето на информация на лице, срещу което е подаден сигнал, докато разследването продължава, може да опорочи самото разследване, като доведе до идентифицирането на сигнализиращото лице. Използването на сигурни и подлежащи на одит системи може да гарантира отчетност и спазване на изискванията за защита на данните. Регулаторните органи следва също така да обмислят въвеждането на многопластов контрол на достъпа и стабилни протоколи за криптиране за защита на чувствителната информация. Периодичните одити от трети страни на тези системи осигуряват допълнително ниво на сигурност, че принципите за защита на данните се спазват. За да се гарантира общественото доверие, външните канали за подаване на сигнали също трябва да наблягат на справедливостта и безпристрастността. Тези мерки демонстрират ангажимент както за защита на данните, така и за отчетност, като укрепват доверието във външните системи за сигнализиране.

3.6.1 Добри практики от Италия

За да се спазят всички горепосочени изисквания на GDPR, в **Италия** Законодателен указ № 24/2023 предвижда, че сигналите не могат да се използват извън необходимото за адекватно проследяване. Самоличността на сигнализиращото лице и всяка друга информация, от която тази самоличност може да бъде изведена, пряко или косвено, не могат да бъдат разкривани без изричното му съгласие на лица, различни от компетентните да получават или проследяват сигналите, изрично упълномощени да обработват такива данни съгласно член 29 и член 32, параграф 4 от Регламент (ЕС) 2016/679⁶² (чл. 12.1). Предвижда се също така, че лични данни, които очевидно не са полезни за обработването на конкретен сигнал, не се събират или, ако бъдат събрани случайно, се изтриват незабавно (чл. 13.2).

Вътрешните и външните сигнали и свързаната с тях документация се съхраняват за времето, необходимо за обработка на сигнала, и във всеки случай не повече от пет години от датата на съобщаване на окончателния резултат от процедурата за подаване на сигнали, съгласно специална разпоредба на **италианското законодателство за защита на данните** (чл. 2-undecies в Законодателен указ № 196 от 30 юни 2003 г., въведен със Законодателен указ № 101 от 10 август 2018 г.).

3.6.2 Намаляване на рисковете за репутацията

Външните канали за сигнализиране също са изправени пред повишени рискове за репутацията, когато чувствителната информация стане публична, както подчертават интервюираните италиански експерти. Разкриването на информация от служителите чрез социалните медии, например, може значително да навреди на репутацията на компанията или публичния орган. Прилагането на строги политики за публично оповестяване и насърчаването на сигурни външни канали за подаване на сигнали могат да намалят тези рискове. Член 11 от италианския Кодекс за поведение подчертава този въпрос, като показва необходимостта от привеждане в съответствие между националните законодателства и разпоредбите на Директивата. За да противодействат на рисковете за репутацията, като същевременно се придържат към принципите на Директивата, организациите могат да предложат множество сигурни и официални начини за подаване на сигнали, включително анонимни горещи линии и криптирани онлайн платформи. Тези канали могат да попречат на сигнализиращите лица да прибегват до социалните медии, като по този начин поддържат поверителността и ограничават щетите върху репутацията.

⁶² Общ регламент относно защита на данните – <https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32016R0679>

3.6.3 Експертиза и обучение

Обратната връзка от интервютата в **Испания** подчертава критичното значение на експертния опит в областта на защитата на данните. Организациите трябва да гарантират, че персоналят, управляващ външни канали за подаване на сигнали, е подходящо обучен и притежава задълбочено разбиране на изискванията на GDPR. Редовните семинари и програми за сертифициране на длъжностни лица по защита на данните (DPO) и друг подходящ персонал могат да засилят спазването на изискванията и да насърчат културата на неприкосновеност на личния живот. Чрез прилагането на тези мерки външните канали за подаване на сигнали могат да постигнат двойната цел за насърчаване на прозрачността и защита на правата на всички участващи страни, насърчаване на доверието и спазването на законовите изисквания.

3.7 ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ

Прилагането на строги технически и организационни мерки е от съществено значение, за да се гарантира спазването на GDPR⁶³ и да се защитят личните данни. Криптирането и псевдонимизацията са широко признати техники, които подобряват сигурността на данните, като правят данните неразбираеми за неоторизирани страни. Контролът на достъпа, базиран на роли, ограничава достъпа до данни до упълномощен персонал, намалявайки риска от неразрешено разкриване.

Организациите трябва да разработят и приложат изчерпателни политики за защита на данните, които очертават ролите, отговорностите и процедурите за обработването на лични данни. Редовните програми за обучение и повишаване на осведомеността на служителите гарантират, че всички заинтересовани страни разбират задълженията си съгласно GDPR и рамките за защита на лицата, сигнализиращи за нередности. Периодичните одити и оценки на риска помагат да се идентифицират уязвимостите и да се гарантира, че мерките за сигурност остават ефективни и актуални.

Плановите за реакция при инциденти са важни за справяне с нарушения на сигурността на данните и минимизиране на тяхното въздействие. Организациите трябва да установят ясни протоколи за откриване, докладване и смекчаване на нарушенията, както и за уведомяване на засегнатите лица и органи, когато е необходимо.

⁶³ Общ регламент относно защита на данните, член 24 – <https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:32016R0679>

3.8 ЗАЩИТА НА ДАННИТЕ ПРИ ПРОЕКТИРАНЕТО И ПО ПОДРАЗБИРАНЕ ПРИ ПУБЛИЧНО ОПОВЕСТЯВАНЕ

Публичното оповестяване е свързано с уникални предизвикателства при балансирането на защитата на данните с необходимостта от прозрачност и отчетност. От съществено значение е начинът, по който организациите спазват задълженията си за защита на лицата, сигнализиращи за нередности в тези случаи. Публичното оповестяване всъщност представлява най-чувствителната форма на подаване на сигнали, при която потенциалът за увреждане на репутацията и правни последици е най-висок. Съгласно Директивата публичното оповестяване се счита за крайна мярка, допустима само когато вътрешните и външните канали за подаване на сигнали са изчерпани или се считат за неефективни. Преди да разкрият информация пред обществеността, организациите (в ролята на външни или вътрешни канали за подаване на сигнали) трябва внимателно да преценят дали оповестяването е в съответствие с принципите на GDPR и служи на обществения интерес. Изричното съгласие следва да се получава, когато е възможно, особено когато става въпрос за чувствителни лични данни.

3.8.1 Роля на защитата на данните при публичното оповестяване

В контекста на публичното оповестяване организациите и лицата, подаващи сигнали за нередности, трябва внимателно да се ориентират в тънката граница между прозрачността и вредата за репутацията. Протоколите за редактиране играят критична роля за защитата на поверителността по време на публично оповестяване. Организациите трябва да премахнат или скрият лични данни, които не са от съществено значение за постигането на целта на разкриването. Това гарантира спазването на принципа на минимизиране на данните, като същевременно защитава правата на физическите лица. Гореспоменатият софтуер GlobaLeaks от **Италия** илюстрира как технологията може да поддържа публично оповестяване. Чрез анонимизиране и криптиране на комуникациите тези платформи позволяват на лицата, подаващи сигнали за нередности, да споделят информация по сигурен начин, намалявайки рисковете, свързани с нерегулираното публично оповестяване. Включването на такава технология в рамките за публично оповестяване може да гарантира спазването на Директивата, като същевременно запази доверието на лицата, сигнализиращи за нередности.

От **Италия** беше изразена загриженост относно потенциалната злоупотреба с публични оповестявания чрез социалните медии. Когато лицата, сигнализиращи за нередности, заобикалят официалните механизми за подаване на сигнали и разкриват чувствителна информация на отворени платформи, това не само застрашава тяхната

поверителност, но и създава значителни рискове за корпоративната или институционалната репутация.

Организациите трябва да информират служителите за правните граници на публичното оповестяване. Член 11б от италианския Кодекс за поведение, например, разглежда небрежното използване на социалните мрежи и подчертава значението на спазването на структурираните механизми за докладване. Допълването на тези мерки с достъпни и стабилни вътрешни и външни канали може да намали вероятността лицата, сигнализиращи за нередности, да прибегнат до публични платформи. В **Италия**, обаче, все още има несъответствие между разпоредбите на Кодекса за поведение и Законодателен указ № 24/2023 относно подаването на сигнали за нередности. Последният изрично признава възможността за публично оповестяване при определени условия, нюанс, който не е адекватно отразен в Кодекса. В същото време липсата на съответствие между Кодекса за поведение и настоящата законодателна рамка създава объркване по отношение на получателя на вътрешни сигнали, тъй като все още неправилно идентифицира йерархичния ръководител вместо отговорника за предотвратяването на корупцията и прозрачността.

3.8.2 Как да се подобри сигурността при публичното оповестяване?

За да приведат публичното оповестяване в съответствие с принципите за защита на данните, организациите и надзорните органи трябва да разработят ясни насоки и защитни мерки. Испанските заинтересовани страни подчертаха значението на защитата на самоличността на лицата, сигнализиращи за нередности, дори при публично оповестяване.

Българската перспектива подчертава важността на ограничаването на достъпа до сигналите до основния персонал. Прилагайки същия принцип към публичното оповестяване, надзорните органи могат да редактират чувствителна информация, която не е от решаващо значение за обществения интерес, като балансират прозрачността със защитата на данните:

За да се предотврати лошо управление на данните при публично оповестяване, се препоръчва регулаторните органи да прилагат строги мерки за предотвратяване на неправилното боравене с данни, като например:

- създаване на протоколи за проверка на точността на оповестяваната информация;
- документиране на всички действия, предприети в отговор на оповестяването.

Прозрачната комуникация за тези процеси успокоява заинтересованите страни и засилва доверието в системата.

3.9 ЦЕНТРОВЕ ЗА ЗАЩИТА НА ДАННИТЕ И ИНФОРМАЦИЯ, ОРГАНИЗИРАНИ ОТ ГРАЖДАНСКОТО ОБЩЕСТВО: ОТВОРЕН ВЪПРОС

В член 20 от Директивата⁶⁴ се признава ролята на „информационните центрове“ като услуги за подкрепа, които гражданското общество може да организира и предоставя, за да помогне на лицата, които биха сигнализирали за нередности, по време на фазата на етични дилеми и общи съмнения относно функционирането на системата. Законът предвижда, че тази роля може да се изпълнява и от специализирани институции.

За да изпълняват тази роля (вижте **Глава 4**), тези информационни центрове задължително влизат в контакт, управляват и съхраняват лични данни, както и друга чувствителна информация.

Гл. 4 >

В тази връзка първоначалната редакция на съображение 89 от Директивата гласи, че информационните центрове **„са обвързани от задължението за запазване на поверителния характер на получената информация“**.

Директивата, обаче, не предоставя допълнителни подробности за това как да се спазва това задължение, дали тези центрове следва да бъдат приравнени на сигнализиращите институции или дали следва да се прилагат специални условия. **Директивата остава неясна по този въпрос**. Тази разлика не е разгледана в достатъчна степен в законодателствата на различните държави, особено като се има предвид, че с редки изключения, подобни услуги за подкрепа все още не са широко практикувани в цяла Европа.

При липсата на конкретни насоки относно практиките за обработване на данни **съществува риск службите за подкрепа да бъдат възпрепятствани да обработват данни**, като по този начин се ограничава способността им да функционират (и потенциално се застрашава способността им да работят изобщо), като същевременно се ограничава достъпът на лицата, които биха сигнализирали за нередности, до подкрепа.

Националните разпоредби или насоки, предоставени от съответните органи за подаване на сигнали за нередности, следва да имат за цел да запълнят тази празнина чрез създаване на ясни протоколи за обработка на данни, които позволяват на лицата, сигнализиращи за нередности, да получават подкрепа, като същевременно изискват от информационните центрове да прилагат надеждни системи за криптиране за получаване, съхраняване (за ограничен период от време) и споделяне на данни между операторите, като по най-добрия начин гарантират защитата и поверителността на информацията на лицата, сигнализиращи за нередности. Както е предвидено в

⁶⁴ Директива (ЕС) 2019/1937 – <https://eur-lex.europa.eu/legal-content/BG/ALL/?uri=CELEX:32019L1937>

съображение 74 от Директивата, служителите на компетентните органи, които отговарят за обработването на сигналите, следва да бъдат професионално обучени, включително относно приложимите правила за защита на данните, за да обработват сигналите и да гарантират комуникация със сигнализиращото лице, както и да проследяват сигнала по подходящ начин.

ОТВОРЕНО УПРАВЛЕНИЕ

Надеждните стратегии за защита на данните са от първостепенно значение за множество заинтересовани страни, като например лицата, подаващи сигнали за нередности, ръководителите на канали за подаване на сигнали, субектите, предлагащи подкрепа на лица, които биха сигнализирали за нередности, като например организациите на гражданското общество, и заинтересованите страни, които имат роля на канал за публично оповестяване, като например журналисти и медии. Тези стратегии следва да включват сигурни механизми за обработка на чувствителна информация, за да се защити самоличността и интересите на сигнализиращите лица. **Междусекторното сътрудничество** с участието на националните регулатори, длъжностните лица по защита на данните и създателите на политики може да бъде от решаващо значение за разработването на иновативни **решения за защита на данните, съобразени с различни сценарии за подаване на сигнали за нередности, особено за справяне със сложността на публичното оповестяване.** Съвместните усилия могат да хармонизират националните законодателства с разпоредбите на Директивата, като разработят ясни насоки за етичното използване на данните, за да се помогне на всички заинтересовани страни да поддържат прозрачност, като същевременно зачитат неприкосновеността на личния живот.

Един все по-важен въпрос, който трябва да бъде разгледан в рамките на отвореното управление, е **обработването на чувствителни и лични данни от консултанти и подкрепящи субекти** – както граждански, така и институционални – както е признато в Директивата. Самата Директива (в съображения разпоредби 89 и 90) задължава тези субекти да гарантират ефективно обработване на данни, въпреки че не предоставя допълнителни подробности.

Помощниците и консултантите, при насочване на лица, които биха подали сигнали за нередности, неизбежно влизат в контакт с чувствителни данни. Тяхната цел не е просто да предоставят обща, деконтекстуализирана информация, а по-скоро да помогнат на хората да се ориентират в правилните канали за подаване на сигнали по смислен начин. Един чисто неутрален, безпристрастен подход не би могъл да отговори на нуждите на лицата, които биха подали сигнали за нередности.

Този въпрос следва да бъде обсъден открито в рамките на отворено управление чрез разработване на ясни насоки, организиране на съвместни дискусии с участието на органите за защита на данните, представители на организации за подкрепа (както граждански, така и институционални) и регулаторни органи, сигнализиращи за нередности.

Целта е да се намери правилният баланс между две ключови нужди: да се гарантира, че лицата, които биха сигнализирали за нередности, получават съдържателни насоки (което може да изисква известно ниво на обработка на данните от службите за подкрепа), като същевременно се зачитават техните лични данни.

Например дискусиите трябва да установят:

- ясни правила за съхранение, включително максимален период на съхранение за чувствителни данни;
- сигурни, поверителни методи за обмен на данни между потенциални податели на сигнали и услуги за подкрепа;
- дефинирани комуникационни протоколи между съветниците в рамките на една и съща услуга.

Ограничително тълкуване, което дава приоритет на неприкосновеността на личния живот над всичко друго, може неволно да подкопае самите интереси на лицата, които биха подали сигнали за нередности, като ограничи способността им да търсят ефективни насоки.

3.10 ПРЕПОРЪКИ

Фондация „Конрад Аденауер“ по време на работата си по различни проекти и политики подчертава, че всеобхватните правни рамки (подобни на GDPR)⁶⁵ са от съществено значение за насърчаване на прозрачността, като същевременно защитават индивидуалните права и ясно определят обхвата и границите на дейностите по подаване на сигнали. Фондацията се застъпва за механизми, които поддържат принципа на пропорционалност при обработването на данни, балансирайки необходимостта от разследване на сигнализираното нарушение с правото на неприкосновеност на личния живот на всички участващи лица. Те също така подчертават значението на кампаниите за повишаване на обществената осведоменост на гражданите и организациите относно техните права и отговорности в рамките на подаване на сигнали за нередности. Изброени са някои практически съвети за прилагане на политиките за защита на данните⁶⁶:

1. СЪЗДАВАНЕ НА НЕЗАВИСИМИ НАДЗОРНИ ОРГАНИ

Създаване на независими надзорни органи, които да наблюдават прилагането на механизмите за подаване на сигнали за нередности, както е определено в приложимата национална правна рамка.

2. АВТОРИТЕТ НА НЕЗАВИСИМИТЕ ОРГАНИ

Тези органи следва да имат правомощия да разследват жалби, да преглеждат практиките за защита на данните и да гарантират спазването на правните стандарти, когато става въпрос за независими органи, които получават жалби по външен канал (или по вътрешен канал).

⁶⁵ Виж също: https://www.kas.de/documents/252038/253252/7_dokument_dok_pdf_47778_2.pdf/c2a538a2-ed3d-1aa7-b2ae-2736329c8a66?version=1.0&t=1539649646584

⁶⁶ Transparency and Accountability [Прозрачност и отчетност] – <https://www.kas.de/en/web/rspno/veranstaltungsberichte/detail/-/content/transparenz-und-rechenschaftspflicht>

3. ЗНАЧЕНИЕ НА ПРОГРАМИТЕ ЗА ОБУЧЕНИЕ

Програмите за обучение както на служителите в публичния, така и в частния сектор са от решаващо значение за повишаване на осведомеността относно протоколите за подаване на сигнали за нередности и принципите за защита на данните.

4. РАБОТА С ПОВЕРИТЕЛНИ ОТЧЕТИ И КОНФИДЕНЦИАЛНОСТ

Служителите трябва да бъдат подготвени да разпознават важността на поверителността, да обработват сигурно чувствителни отчети и да избягват неоторизирани разкривания.

5. ДОБРИ ПРАКТИКИ ЗА ЗАСИЛВАНЕ НА СЪОТВЕТСТВИЕТО

Като цяло, ето няколко добри практики, които организациите могат да следват, за да засилят съответствието си и да насърчат доверието:

5.1 РАЗРАБОТВАНЕ НА ПОДРОБНИ ПОЛИТИКИ ЗА ПОДАВАНЕ НА СЪОБЩЕНИЯ

Организациите трябва да разработят подробни политики, които очертават целта, обхвата и процедурите на техните системи за подаване на сигнали. Тези политики трябва да отговарят на изискванията за защита на данните, включително събиране, съхранение, обработка и съхранение на данни. Като правят тези политики достъпни за всички заинтересовани страни, организациите демонстрират прозрачност и отчетност.

5.2 НАЗНАЧАВАНЕ НА ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ (DPO)

Назначаването на квалифицирано длъжностно лице по защита на данните (DPO) е от решаващо значение за гарантиране на текущото съответствие с GDPR и Директивата за лицата, сигнализиращи за нередности. DPO могат да предоставят насоки относно обработването на лични данни, да извършват одити и да служат като точка за контакт за субектите на данни и надзорните органи.

5.3 СПЕЦИАЛИЗИРАНИ ПРОГРАМИ ЗА ОБУЧЕНИЕ КЪМ ЗАИНТЕРЕСОВАНИТЕ СТРАНИ

Програмите за обучение следва да бъдат съобразени с нуждите на различните групи заинтересовани страни, включително служители, ръководители и външни доставчици на услуги. Тези програми трябва да подчертаят значението на поверителността, минимизирането на данните и правата на субектите на данни. Обучението, базирано на сценарии, може да помогне на служителите да разберат как да се справят ефективно с чувствителни случаи на подаване на сигнали.

5.4 ВЪВЕЖДАНЕ НА СИГУРНИ КАНАЛИ ЗА ДОКЛАДВАНЕ

Организациите следва да въведат сигурни и лесни за използване канали за подаване на сигнали, които позволяват на сигнализиращите лица да подават информация поверително. Многофакторното удостоверяване и криптираните комуникационни протоколи могат да подобрят сигурността на тези системи. Освен това организациите трябва редовно да тестват тези системи, за да идентифицират и адресират уязвимостите.

5.5 ПЕРИОДИЧЕН МОНИТОРИНГ И ОДИТ

Периодичният мониторинг и одит на системите за подаване на сигнали помагат да се гарантира спазването на изискванията за защита на данните. Организациите следва да поддържат подробна документация за дейностите по обработване на данни, включително обосновка за събирането и съхранението на данни. Одитите могат да идентифицират пропуски в съответствието и да предоставят възможности за непрекъснато подобрене.

5.6 АНГАЖИРАНЕ С РЕГУЛАТОРНИТЕ ОРГАНИ

Сътрудничеството с националните органи за защита на данните и други регулаторни органи може да помогне на организациите да бъдат информирани за промените в законодателството и най-добрите практики. Сътрудничеството също така улеснява разрешаването на сложни случаи, като например тези, свързани с трансгранично предаване на данни или конфликти между националните разпоредби и разпоредбите на ЕС.

5.7 ИЗПОЛЗВАНЕ НА ИНОВАТИВНИ ТЕХНОЛОГИИ

Иновативните технологии, като изкуствен интелект и машинно самообучение, могат да повишат ефективността и сигурността на системите за подаване на сигнали. Например, инструментите, задвижвани от AI, могат да откриват модели на неправомерно поведение, да идентифицират нарушения на данните и да поддържат процеси на анонимизиране. Организациите обаче трябва да гарантират, че тези технологии отговарят на GDPR и други приложими разпоредби.

5.8 УСТАНОВЯВАНЕ НА МЕТРИКИ ЗА ЕФЕКТИВНОСТ

Организациите следва да установят показатели за оценка на ефективността на своите системи за подаване на сигнали, включително степента на разрешаване на сигнализираните случаи, нивата на удовлетвореност на сигнализиращите лица и цялостното спазване от страна на организацията на стандартите за защита на данните. Редовното отчитане на тези показатели може да изгради доверие сред заинтересованите страни и да подчертае областите за подобрене (вижте [Глава 5](#) за допълнителна информация).

5.9 НАСЪРЧАВАНЕ НА НЕПРЕКЪСНАТО ПОДОБРЯВАНЕ

Защитата на данните е непрекъснат процес, който изисква от организациите да се адаптират към променящата се правна, технологична и обществена среда. Чрез насърчаване на култура на непрекъснато усъвършенстване, организациите могат да гарантират, че техните системи за подаване на сигнали остават ефективни, сигурни и съвместими с променящите се стандарти. Чрез включването на тези стратегии/добри практики организациите, както и националните правителства, могат да създадат механизми за подаване на сигнали за нередности, които са както в съответствие със закона, така и на практика ефективни. Тези системи не само насърчават хората да сигнализират за неправомерно поведение уверено, но също така укрепват цялостното управление, повишават общественото доверие и допринасят за култура на почтеност.

5.10 БАЛАНСИРАНЕ НА ОБЩЕСТВЕНИЯ ИНТЕРЕС С ПРАВАТА ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИЯ ЖИВОТ

Балансирането на обществения интерес с правата на неприкосновеност на личния живот изисква оценка на пропорционалността, като се вземат предвид фактори като сериозността на сигнализирания проблем, потенциалното въздействие на оповестяването и наличието на алтернативни решения. Организациите трябва да документират своите процеси на вземане на решения, за да демонстрират отчетност и съответствие с регулаторните изисквания, като вътрешни регистри, правила и процедури, кодекси за поведение, както и етични кодекси.

5.11 ДАВАНЕ НА ПРИОРИТЕТ НА ПОВЕРИТЕЛНОСТТА НА ЛИЦАТА, ПОДАВАЩИ СИГНАЛИ ПРИ ПУБЛИЧНО РАЗКРИВАНЕ

Механизмите за публично разкриване трябва да дават приоритет на поддържането на поверителността на лицата, сигнализиращи за нередности, освен ако не е предоставено изрично съгласие. Организациите следва да установят ясни и достъпни процедури, за да могат лицата, сигнализиращи за нередности, да изразяват своите предпочитания по отношение на оповестяването и да гарантират, че тези предпочитания се спазват.

5.12 ИЗВЪРШВАНЕ НА ОЦЕНКИ НА РИСКА ПРЕДИ ПУБЛИЧНО ОПОВЕСТЯВАНЕ

За публичното оповестяване следва да се въведат стабилни рамки за оценка на риска, за да се оценят потенциалните последици от публикуването на информация. Това включва оценка на вероятността от вреда за сигнализиращите лица, замесените лица или обществеността. Когато е възможно, към данните следва да се прилагат техники за анонимизиране и псевдонимизация преди оповестяването.

5.13 ИЗПОЛЗВАНЕ НА ИНСТРУМЕНТИ ЗА АВТОМАТИЗИРАНО РЕДАКТИРАНЕ

Използването на технологични решения, като например автоматизирани инструменти за редактиране, може да рационализира подготовката на данните за публично оповестяване. Тези инструменти могат да откриват и маскират чувствителна лична информация последователно и ефективно, минимизирайки риска от човешка грешка.

5.14 УСТАНОВЯВАНЕ НА КРИТЕРИИ ЗА ПУБЛИЧНО ОПОВЕСТЯВАНЕ

Организациите трябва също така да установят ясни критерии за определяне кога е целесъобразно публичното оповестяване. Факторите, които трябва да се вземат предвид, включват спешността на проблема, наличието на вътрешни или външни механизми за сигнализиране и потенциалните ползи и рискове от оповестяването.

5.15 ОБУЧЕНИЕ НА ПЕРСОНАЛ, УЧАСТВАЩ В ПУБЛИЧНО ОПОВЕСТЯВАНЕ

На последно място, програмите за образование и обучение на персонала, участващ в процесите на публично оповестяване, са от съществено значение. Тези програми следва да обхващат правните и етичните аспекти на защитата на данните, значението на баланса между неприкосновеността на личния живот и прозрачността, както и техническите умения, необходими за работа с чувствителна информация.



Защита и подкрепа на лицата, подаващи сигнали за нередности



ГЛАВА 4

ЗАЩИТА И ПОДКРЕПА НА ЛИЦАТА, ПОДАВАЩИ СИГНАЛИ ЗА НЕРЕДНОСТИ

ГЛАВА 4

4.1 ЗАЩИТА, ПРЕДВИДЕНА В ДИРЕКТИВА 2019/1937/ЕС

Директивата предоставя цялостна защита на лицата, които подават сигнали за нарушения на правото на Съюза, като гарантира, че широк спектър от лица, участващи в дейности, свързани с работата, са защитени от ответни действия с цел отмъщение. Тази защита се простира отвъд традиционните работници и служители и обхваща широк кръг от лица:

- държавни служители, както и самостоятелно заети лица, като например лица на свободна практика и независими изпълнители (съгласно член 49 от ДФЕС);
- акционери и членове на управителния съвет без изпълнителни функции;
- доброволци и стажанти, независимо дали са платени или неплатени;
- бивши работници;
- помощници – физически лица, които при спазване на конфиденциалност помагат на лицата, подаващи сигнали за нередности. Те могат да бъдат правни съветници, предлагащи стратегически насоки, представители на синдикатите, които се застъпват за лицата, подаващи сигнали, и други доверени посредници, които помагат да се ориентират в сложността на разкриването;
- трети страни, които могат да претърпят ответни мерки поради връзката си с лицето, сигнализиращо за нередности, включително членове на семейството, колеги и дори юридически лица, свързани със сигнализиращото лице.

Защитата на сигнализиращи лица **не се прилага** за лица, които разкриват информация директно на пресата, освен в случаите, когато националното законодателство установява специална защита на свободата на изразяване на мнение и свободата на информация (член 15, параграф 2). В резултат на това **журналистите са изключени от защитата на Директивата**.

В **България** в защитата по дела срещу журналисти се правят опити за включване на аспекти от концепцията за стратегически съдебни производства, насочени срещу публично участие (SLAPP) и законодателството за защита на лицата, сигнализиращи за нередности.

Налага се мнението обаче, че са необходими решения на законодателно равнище (в правото на ЕС и националното право), както и практически действия в посока „защитата на свободата на изразяване в стратегически дела срещу публично участие да върви ръка за ръка със защитата на лицата, сигнализиращи за нередности“. Въз основа на това съображение следва да се има предвид, че защитата **остава валидна независимо** от избрания канал, стига оповестяването да е в съответствие с разпоредбите на Директивата. Ако **вътрешните или външните** механизми се окажат неефективни или ако има непосредствена заплаха за обществения интерес, лицата, подаващи сигнали за нередности, могат да оповестят публично своите опасения, без да губят **правното си основание** за защита.

Различните заинтересовани страни обаче **възприемат вътрешните канали** като **по-малко сигурни от външните**, особено когато сигналите са в конфликт с интересите на организацията. Мнозина се страхуват от отмящение. Това безпокойство **се отнася до персонала, натоварен с получаването и обработването** на сигнали, който – поне в **Италия** – често не е независим от своите организации и не се ползва с необходимите гаранции, които биха им позволили да изготвят сигнали ефективно.

4.1.1 Какво трябва да направи лицето, сигнализиращо за нередности, за да отговаря на условията за защита?

За да се ползват от предвидената защита съгласно Директивата, **лицата, сигнализиращи за нередности, трябва да отговарят на специфични условия**, а именно да подават сигналите по подходящи канали и да имат **основателно убеждение**, че разкритата информация е вярна. Директивата не позволява субективни оценки на мотивите на сигнализиращото лице да съобщи за нарушение. Следователно **„добросъвестността“** не е релевантен фактор; най-важното е лицето, сигнализиращо за нередности, **основателно да вярва**, че е извършено или е вероятно да бъде извършено нарушение. Тази концепция, наричана основателно убеждение, заменя традиционния стандарт за добросъвестност.

Какво представлява „основателно убеждение“?

- **Основателното убеждение** се гради на обективни, конкретни елементи, като доказателства или проверими улики, които карат сигнализиращото лице да вярва, че представените факти са верни. Това означава, че дори ако оповестената информация по-късно се окаже невярна, сигнализиращото лице остава защитено, докато е имало разумни основания да я счита за вярна към момента на подаване на сигнала. Тази предпазна мярка е от решаващо значение за насърчаване на хората да излязат наяве, без да се страхуват от наказание за непреднамерени грешки.
- **Личният мотив** на сигнализиращото лице е **без значение** за неговата защита. Този принцип е потвърден отново в **съображение**

32 от Директивата, както и в Резолюция 10/8 на Конвенцията на Организацията на обединените нации срещу корупцията (UNCAC) „Защита на сигнализиращите лица“, точка 14. След 2019 г. е налице **окончателна промяна от оценка на личните мотиви на лицето, сигнализиращо за нередности, към оценка на обективните факти в самия сигнал**. Принципът на основателност също играе решаваща роля за предотвратяване на злонамерени сигнали (т.е. явно неверни твърдения), които биха могли да навредят несправедливо на физически лица или организации. Въпреки това, Европейската конвенция за правата на човека (ЕКПЧ) продължава да включва добросъвестността като изискване за защита, което явно е в конфликт с Директивата.

Важното е, че сигналите се подават в публичен интерес или в интерес на почтеността на публичната администрация или частния субект: причините, които са накарали едно лице да подаде сигнал, да разобличи нещо или да оповести публично информация, са без значение за целите на неговата защита.

Защита при анонимно подаване на сигнали

За да се гарантира защита, сигнализиращите лица трябва да използват каналите за подаване на сигнали, описани в **Глава 2**.

Гл. 2 >

Директивата признава, че анонимните сигнали могат да спомогнат за изграждането на доверие в системите за подаване на сигнали за нередности. Сигнализиращите лица, които изберат да подадат сигнал анонимно и по-късно да разкрият самоличността си, могат да получат защита, ако са заплашени от ответни действия (член 6, параграф 3). Въпреки това, подходите към анонимните сигнали варират в отделните три държави, участващи в този проект, и като цяло в Европа.

Италианското законодателство не регламентира анонимни сигнали, с изключение на предоставянето на защитата на анонимни сигнализиращи лица, които са подложени на ответни действия с цел отмъщение. Националният орган за борба с корупцията (ANAC), който управлява **външния канал**, третира анонимните сигнали като обикновени жалби, докато не бъде задействана защитата. Ако анонимно лице, сигнализиращо за нередности, по-късно се сблъска с ответни действия, то има право на същата защита като неанонимните **сигнализиращи лица (чл. 6 от Законодателен указ № 24/2023)**. Ключова разлика по отношение на анонимното подаване на сигнал е, че достъпът до сигнала се счита за разрешен при специфични условия и ограничения, установени от италианското законодателство. Това е така, защото анонимните жалби се третират като обикновени жалби съгласно общите правни разпоредби: а) документален и защитен достъп (членове 22 и сл. от Закон № 241/1990) и б) граждански достъп (членове 5 и следващите от Законодателен указ № 33/2013).

България не регулира официално анонимното подаване на сигнали. Въпреки това лицата, които са подали анонимни сигнали или анонимно са разкрили публично информация за нарушения, и които впоследствие са **идентифицирани и са станали обект на ответни действия, имат право на защита (член 10 от Закона за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения).**

Испания позволява анонимно подаване на сигнали и предоставя **защита на лицата, сигнализиращи за нередности, които по-късно са идентифицирани и са станали обект на ответни действия с цел отмъщение (член 7, параграф 3 за вътрешно подаване на сигнали и член 17 за външно подаване на сигнали, Закон № 2/2023 от 20 февруари 2023 г.).** Съгласно испанското законодателство нарушаването на гаранциите за поверителност и анонимност представлява много сериозно нарушение в рамките на режима на санкциониране. Всяко действие или бездействие, насочено към разкриване на самоличността на сигнализиращо лице, което е избрал анонимност, е забранено – дори и да не се стигне до действителното разкриване.

4.2 МЕРКИ ЗА ПОДКРЕПА ОТ ЗАДЪЛЖЕНИТЕ СУБЕКТИ

Първата мярка за подкрепа (член 20 от Директивата) е предлагането на изчерпателна и независима информация и съвети, които са лесно достъпни за обществеността и безплатни. Това включва насоки относно: а) наличните процедури и средства за правна защита, б) защитата срещу ответни действия с цел отмъщение и в) правата на засегнатото лице. Освен това лицата, сигнализиращи за нередности, следва да получават ефективна помощ от компетентните органи пред всеки съответен орган, свързан с тяхната защита срещу ответни действия с цел отмъщение. Това включва:

- удостоверяване, когато е предвидено в националното законодателство, потвърждаващо, че те отговарят на условията за закрила;
- правна помощ при наказателни и трансгранични граждански производства в съответствие с Директива (ЕС) 2016/1919 и Директива 2008/52/ЕО на Европейския парламент и на Съвета;
- допълнителна правна помощ, правни консултации или друга правна помощ при по-нататъшни производства, когато това е разрешено от националното законодателство.

4.2.1 Роля на органите

- **Компетентните органи** трябва активно **да подкрепят лицата, сигнализиращи за нередности**, които са обект на ответни действия с цел отмъщение, изпълнявайки функциите на тяхна първа точка за контакт.

- Лицата, сигнализиращи за нередности, следва да докладват за положението си на тези органи, които **отговарят за прилагането на Директивата** в рамките на тяхната държава членка.
- Органите преценяват дали лицето **отговаря на критериите за защита** и дали е обект на ответни действия.
- Органите трябва да гарантират, че лицата, сигнализиращи за нередности, получават подходящо правно признаване и помощ.

4.1.2 Форми на подпомагане, предвидени в Директива 2019/1937/ЕС

В съображение 90 от Директивата се предвижда, че **компетентните органи** следва да предоставят на лицата, сигнализиращи за нередности, необходимата подкрепа за ефективен достъп до защита. По-специално, те следва: а) да предоставят **доказателства или друга документация**, потвърждаваща пред други органи или съдилища, че е **извършено външно сигнализиране**, и б) да гарантират, че лицата, сигнализиращи за нередности, разбират **своите права и наличните ресурси**.

Търсенето на **професионални съвети** може да осигури увереността, необходима за навигиране в процеса, като същевременно гарантира най-високо ниво на защита съгласно закона.

Правни действия срещу отмъщение

Следва да има безплатна и **независима правна помощ**, която да помогне на лицата, подаващи сигнали за нередности, да се ориентират в процесите на подаване на сигнали и да разберат правата си. Някои юрисдикции разширяват обхвата на правната помощ както за **граждански, така и за наказателни производства**, включващи дела за защита на сигнализиращите лица. Ако лицето, сигнализиращо за нередности, **се сблъска с ответни действия** – като уволнение, понижаване или тормоз – то има право да **потърси правни средства за защита**, включително временни мерки и пълно обезщетение (член 21, параграф 8).

За да подкрепят твърдението си, сигнализиращите лица **трябва да представят доказателства**, показващи, че са подали сигнал и че срещу тях са предприети ответни действия. **Националните съдилища и трибунали** играят решаваща роля за **прилагането на ефективна защита**, като гарантират, че на засегнатите лица ще бъде възстановен предишният статут и ще получат обезщетение за претърпените вреди.

В съдебно⁶⁷ производство относно вреди, претърпени от сигнализиращо лице, ако последното докаже, че е съобщило за нарушение и е претърпяло вреда, се приема, че вредата е резултат от ответни действия. В такива случаи тежестта на доказване се прехвърля

⁶⁷ Чл. 38.4 испански закон № 2/2023, чл. 37 от българския закон, чл. 19 от италианския закон № 24/2023.

върху страната, която е предприела неблагоприятни мерки, тя трябва да докаже, че предприетото действие се основава на надлежно обосновани основания.

Пример от практиката в Испания: създаден е фонд за безплатна правна, социална и психологическа подкрепа за лицата, подаващи сигнали за нередности. В **Холандия** има подобна инициатива. Във **Франция** лицата, подаващи сигнали за нередности, могат да получат средства за съдебни разноски и субсидии при обжалване на ответни мерки или при защита срещу правни действия, целящи да възпрепятстват подаването на сигнала или публичното оповестяване на информация.

Интересно е да се отбележи, че в **Италия** в случаи на опит за или заплахата от ответни действия транспониращият закон предвижда, че лицето, сигнализиращо за нередности, трябва да представи данни, показващи вероятността („*fumus*“) от заплахата или опита за ответни действия. Едва след това тежестта на доказване се прехвърля върху страната, обвинена в ответни действия, като се изисква тя да докаже, че предполагаемите действия не са свързани със сигнала, подаден от сигнализиращото лице. Това е обратното на тежестта на доказване, предвидена в Директивата като задължителна. В **Италия** това е предвидено в транспониращото законодателство, което не се изисква от Националния орган за борба с корупцията (ANAC).

В допълнение към правната помощ, лицата, сигнализиращи за нередности, **могат да получат психологическа и финансова подкрепа**, особено когато ответните действия причиняват емоционален стрес и/или икономически затруднения. В някои случаи властите могат официално да признаят статута на лицето, сигнализиращо за нередности, засилвайки неговата правна защита и надеждност.

Достъп до услуги за подкрепа

За да се защитят допълнително лицата, сигнализиращи за нередности, държавите членки могат да създават независими консултантски служби и центрове, които предоставят правна помощ, практически насоки, информация и подкрепа. Лицата, подаващи сигнали за нередности, могат да се обърнат към тези услуги за поверителен съвет относно техните права, налични средства за защита и правни възможности. Тези структури за подкрепа са предназначени да овластяват хората, като гарантират, че те могат да се ориентират в процеса на сигнализиране и защита с увереност. Съгласно Директивата тези услуги могат да се предоставят от публична институция или от граждански субекти.

Испанското законодателство изрично позволява ефективна помощ от всеки съответен орган, свързан със защитата на лицата, подаващи сигнали за нередности, от ответни действия с цел отмъщение,

включително издаването на удостоверение, потвърждаващо правото им на защита съгласно закона.

Отмъщение извън работното място

Ответните действия срещу лицата, подаващи сигнали за нередности, се простират отвъд последиците на работното място като уволнение или понижаване. Те могат да включват и:

- тормоз и сплашване;
- репутационни щети;
- кампании за оклеветяване в социалните медии;
- черни списъци в сектора или отрасъла, които могат сериозно да повлияят на перспективите за кариера на подателя на сигнал.

Директивата изрично разглежда тези рискове, като гарантира защита извън работното място и признава, че лицата, сигнализиращи за нередности, могат да се сблъскат с по-широки обществени последици.

Италианското законодателство изрично гарантира защита, обхващаща и ответните действия, които могат да се състоят в икономически или финансови вреди, включително загуба на икономически възможности и загуба на доходи; предсрочно прекратяване или разваляне на договора за доставка на стоки или услуги; анулиране на лиценз или разрешение; необосновано искане за психиатрични или медицински прегледи.

Удостоверяване от компетентните органи

В редица държави членки официалният статут на лице, сигнализиращо за нередности, е предпоставка за получаване на подкрепа и защитни мерки. В някои държави членки статутът на сигнализиращото лице се признава при предоставянето на съответно „удостоверяване“, както е посочено в съображение 90, параграф 1 от Директивата. Сред страните, които са въвели такова удостоверяване, са Франция, Латвия, Полша и **Испания**, в частност от Агенцията за предотвратяване и борба с измамите и корупцията на региона на Валенсия (AVAF). Този вид удостоверяване служи като официално признаване на техния статут и може да бъде полезно в съдебни производства или при търсене на помощ от публични или частни институции. Това укрепва техните аргументи, когато трябва да докажат правото си на защитни мерки.

Съгласно **определени национални рамки лицата, сигнализиращи за нередности, могат да отговарят на изискванията за удостоверяване**, което потвърждава, че те отговарят на законовите изисквания за защита. Въпреки това, дори при липса на удостоверяване, лицата, сигнализиращи за нередности, следва да имат ефективен достъп до **съдебен контрол**. Съдилищата в крайна сметка ще решат – въз основа на всички индивидуални обстоятелства по случая, дали лицето,

сигнализиращо за нередности, отговаря на условията за защита съгласно приложимите правила.

4.3 РАЗШИРЯВАНЕ НА ОБХВАТА НА НАРУШЕНИЯТА

Въпреки че Директивата се съсредоточава предимно върху нарушенията на правото на ЕС, тя насърчава държавите членки да разширят обхвата на защитата, така че да включва нарушения на националното законодателство и при неетично поведение, което, макар и да не е незаконно, създава рискове за обществото. Чрез разширяване на обхвата на защитените оповестявания на информация държавите членки могат да засилят гаранциите за лицата, сигнализиращи за нередности, като гарантират по-голяма защита срещу неправомерно поведение, което може да навреди на обществения интерес, демокрацията или институционалната почтеност.

РАВЕНСТВО МЕЖДУ ПОЛОВЕТЕ

Защитата на лицата, подаващи сигнали за нередности, изисква **приобщаващ подход**, като се признава, че хората от **маргинализирани групи** или тези, които са изправени пред междусекторни уязвимости, могат да изпитат **по-висок риск от отмъщение** и по-голям страх от другите. Рискът от отмъщение **може да повлияе** на това дали и как човек решава да подаде сигнал. Изследвания, включително проучвания, проведени от Асоциация „Прозрачност без граници“ (Transparency International), потвърждават, че жените могат да изпитват по-голям страх и стрес, когато съобщават за неправомерно поведение (вижте карето за равенство между половете в **глава 5**).

Един от основните фактори, влияещи върху решението на жените да сигнализират за неправомерно поведение, е динамиката на управлението на работното място:

- Дисбаланс на управлението в организацията: работната среда често е доминирана от мъже на властови позиции и правомощия за вземане на решения. Колкото по-голям е **дисбалансът на властта** между мъжете и жените, толкова по-голям е рискът от отмъщение за жените, подаващи сигнали за нередности.
- Отмъщението срещу жените често е насочено към тяхната лична сфера: за разлика от други форми на отмъщение, жените могат да бъдат подложени на **интимни и лични атаки**, като сексистки коментари или тормоз, основан на пола.
 - България: организациите на гражданското общество изразяват загриженост относно нарастващия брой съдебни искове срещу жени в журналистиката. Жените журналисти често се възприемат като по-слабия пол, което ги прави по-лесни мишени за сплашване и тактики на страх.
- Здравно и психологическо въздействие: изследванията показват, че жените вземат **отпуск по болест** по-често от мъжете, след като съобщават за неправомерно поведение, често като начин да се избегне отмъщение на работното място.
 - Италия: проучванията показват, че неблагоприятните условия, пред които са изправени жените при подаването на сигнали за нередности, се проявяват и в **по-ниска осведоменост** за техните права и намалена способност да се защитават в съдебни производства.

Гл. 5 >

За да се справят с тези предизвикателства, свързани с пола, организациите следва:

■ **Да разработят и одобрят протоколи за чувствителни към аспектите на пола сигнализиращи лица (вижте карето в **Глава 1**):**

- С консенсус и адекватно представителство организациите следва да създадат специфични протоколи или насоки за разглеждане на случаи на подаване на сигнали за нередности, свързани с пола.
- Те трябва да гарантират, че тези протоколи са интегрирани както в политиките за защита на лицата, сигнализиращи за нередности, така и в политиките за равенство и недискриминация на организацията.
- Тези протоколи следва да очертаят ясни процедури за сигнализиране, разследване и справяне със случаи на насилие, тормоз или дискриминация, основани на пола.
- Всички лица следва да бъдат напълно информирани за правата си и наличните услуги за подкрепа.

■ **Да разширят достъпа до правна помощ, психологическа подкрепа, както и външни услуги:**

- Да осигурят правна помощ, която е широко достъпна за жените и други групи, изложени на дискриминация, така че те да могат да се защитават по-добре срещу ответни мерки с цел отмъщение и правни действия.
- Да проектират механизмите за сигнализиране така, че да предотвратяват ответни действия и повторно виктимизиране в случаи, основани на пола, като се гарантира, че сигналите не могат да бъдат достъпни за лица в една и съща йерархия на работното място, като например ръководители или колеги. Лицата, подаващи сигнали за нередности, трябва да се чувстват сигурни, че тяхната самоличност и действия ще бъдат защитени, особено в чувствителни случаи, основани на пола, когато рискът от ответни действия е по-висок.
- Да предоставят информация за външни услуги за подкрепа, включително правна помощ, психологическа подкрепа и за организации за защита на лица, преживели насилие. Това позволява на лицата, които биха подали сигнали за нередности, да се чувстват по-сигурни и информирани, когато обмислят дали да сигнализират за неправомерно поведение и да се сблъскат с предизвикателствата, които ги очакват по време на процеса.

Гл. 1 ➤

В **Испания** например, **защита се предоставя на физически лица, които съобщават както за действия или бездействия, предвидени в материалния обхват** на Директивата, така и за действия или бездействия, които могат да представляват сериозно или много тежко престъпление или административно нарушение съгласно испанската правна система, като „всички онези тежки или много тежки престъпления или административни нарушения, които водят до икономически загуби за държавната хазна и за социалното осигуряване се считат включени“ (чл. 2.1, буква б) от Закон № 2/2023).

4.4 ПУБЛИЧНО ОПОВЕСТЯВАНЕ И ИЗВЪНРЕДНИ СИТУАЦИИ

Лицата, подаващи сигнали за нередности, обикновено се насърчават да използват каналите за вътрешно или външно сигнализиране, преди да оповестят публично информацията си. Те обаче остават защитени, ако е необходимо публично оповестяване (съгласно член 15 от Директивата) поради непосредствени заплахи – като екологични бедствия, рискове за здравето или финансови измами – или ако доказателствата могат да

бъдат унищожени или органите са компрометирани⁶⁸. В **Испания**, лицата, сигнализиращи за нередности, трябва да отговарят на **специфични изисквания**, за да получат защита при публично **оповестяване**. Тези изисквания следва да бъдат подробни, а не да се разчита на обща информация.

4.5 ЗАГУБА НА ЗАЩИТА

Защитата може да бъде отменена при определени условия, за да се предотврати злоупотреба, като същевременно се запази целостта на системата:

- **Злонамерени сигнали:** лицата, подаващи сигнали за нередности, които съзнателно предоставят невярна или подвеждаща информация, губят защитата си; държавите членки могат да налагат санкции за такива случаи.
- **Неспазване на процедурите:** подаването на сигнали извън определените канали обикновено води до загуба на защита, освен в случаите на спешни заплахи или унищожаване на доказателства.
- **Незаконни дейности:** лицата, подаващи сигнали за нередности, участващи в манипулиране на компютърни системи и мрежи, кражба на данни или неоторизиран достъп, не са защитени, за да се гарантира отговорно използване на системата.
- **Нарушаване на поверителността:** ако лицето, сигнализиращо за нередности, разкрие прекомерна или чувствителна информация без основание, защитата може да бъде отменена.
- **Неправилно публично оповестяване:** лицата, подаващи сигнали за нередности, трябва първо да се опитат да сигнализират чрез вътрешните или външните канали, освен ако не е надлежно обоснована необходимостта от спешно публично оповестяване.

4.6 ПОДКРЕПА ЗА СИГНАЛИЗИРАЩИ ЛИЦА: КОЙ МОЖЕ ДА ПОМОГНЕ?

Директивата (съображение 41 и след това член 4) разширява защитата на лицата, които помагат на лицата, сигнализиращи за нередности, като гарантира, че всички участници могат да работят безопасно и ефективно.

⁶⁸ Съгласно испанското законодателство лице, което прави публично оповестяване, отговаря на условията за защита съгласно закона, „ако са изпълнени условията за защита, уредени в раздел VII, и някое от следните условия:

а) че е осъществило комуникацията първо по вътрешни и външни канали или директно по външни канали в съответствие с раздели II и III, без да са предприети подходящи действия по този въпрос в определения срок;

б) че има разумни основания да смята, че нарушението може да представлява непосредствена или явна опасност за обществения интерес, по-специално когато е налице извънредна ситуация, или съществува риск от необратими вреди, включително опасност за физическата неприкосновеност на дадено лице; или, в случай на комуникация чрез външен информационен канал, съществува риск от ответни действия или има малка вероятност информацията да бъде обработена ефективно поради конкретните обстоятелства по случая, като например укриване или унищожаване на доказателства, тайно споразумение на орган с извършителя на нарушението или че органът е замесен в нарушението.

Условията за защита, предвидени в предходната алинея, не се прилагат, когато лицето е разкрило информация директно на пресата в съответствие с упражняването на свободата на изразяване на мнение и вярна информация, предвидена в Конституцията и законодателството за нейното прилагане (чл. 28, Закон № 2/2023).

Помощници

Помощниците, например правни съветници и представители на синдикатите, помагат на лицата, подаващи сигнали за нередности, да съобщават за нарушения по сигурен начин. Тяхната роля включва:

- предоставяне на правни насоки;
- гаранции за спазването на процедурите за докладване;
- поддържане анонимността на лицата, сигнализиращи за нередности.

Член 2.1 от италианския закон определя помощника като „лице, което подпомага подателя на сигнал в процеса на подаване на сигнал, работещо в същия контекст и чиято помощ трябва да бъде поверителна“. Помощта, предлагана от помощника, може да се състои в съвет или подкрепа за сигнализиращото лице. Например, помощникът може да бъде колега на сигнализиращото лице, който му помага по поверителен начин.

Чл. 5, ал. 4 от българския закон предвижда, че защита се предоставя и на „лица, които помагат на сигнализиращото лице в процеса на подаване на сигнал и чиято помощ следва да е поверителна“. Законът не нарича тези лица „помощници“ и не предоставя никакви подробности за това в какво може да се състои тази помощ.

Испанското законодателство изрично признава помощниците като защитени лица. Съгласно чл. 3.3 от закона: „Настоящият закон обхваща и физическите лица, които подпомагат сигнализиращия в процеса, включително тези, които оказват подкрепа в работната среда, и тези, които са свързани с него и могат да бъдат подложени на репресии в трудова или професионална среда, както и юридическите лица, собственост на сигнализиращия, за които той работи или с които поддържа отношения в трудова среда или в които има значително участие. Това включва посредници като: правни съветници, синдикални представители, колеги и лица, предоставящи психологическа или институционална подкрепа“.

Тяхната защита има за цел да предотврати непряко отмъщение и да гарантира, че сигнализиращият може да действа безопасно, особено в чувствителна работна среда. Това разширяване на субективния обхват на защитата отговаря на разпоредбите на съображение 41 и член 4 от директивата, като гарантира, че всички лица, участващи добросъвестно в процеса на сигнализиране, могат да действат без страх от негативни последици.

Организации на трети лица

Неправителствените организации и групите на гражданското общество могат да:

- предлагат подкрепа на лица, които биха подали сигнали, действайки като информационни центрове (вж. по-долу), чрез предоставяне на практически съвети относно подаването на сигнали и законовите права, помощ при подаване на сигнали, психологическа подкрепа за подпомагане на сигнализиращите лица да се справят със стреса и обществената реакция;
- предлагат безопасни канали и публичност на оповестяването, улесняване на достъпа до медиите или създаване на условия за публикуване чрез независими платформи.

Компетентни органи

Определени от държавата органи, които:

- насочват лицата, сигнализиращи за нередности, относно процедурите за подаване на сигнали;
- обясняват механизмите за защита;
- удостоверяват статута на лице, сигнализиращо за нередности, когато е приложимо, за предотвратяване на ответни действия с цел отмъщение.

Информационни центрове

Независимите административни органи служат като центрове за подкрепа на лицата, сигнализиращи за нередности, предлагайки правни съвети, консултации и координация на наличните ресурси. Организациите на гражданското общество също могат да изпълняват тази роля. В **Италия** законът отрежда решаваща роля на организациите от третия сектор в подкрепата на лицата, сигнализиращи за нередности. Организациите предоставят безплатно информация, съдействие и съвети относно начина на сигнализиране и защитата от ответни действия с цел отмъщение, предлагана от националното законодателство и законодателството на ЕС, относно правата на засегнатите лица и относно реда и условията за достъп до правна помощ.

Колеги и ръководители, оказващи подкрепа

Доверените колеги или ръководители могат да:

- осигуряват неформална подкрепа;
- помагат за прецизирането на сигналите, за да се осигури точност;
- съдействат за правилното използване на вътрешните канали за подаване на сигнали.

Лица, предоставящи правна помощ

Както публичните, така и частните организации, предоставящи правна помощ, помагат на лицата, сигнализиращи за нередности, които са изправени пред отмъщение, като ги подкрепят в съдебни производства, за да търсят обезщетение или да защитят правата си.

Психологическа и социална подкрепа

Лицата, които биха подали сигнали, но не са сигурни как да направят това или дали в крайна сметка ще бъдат защитени, могат да бъдат обезкуражени да подават сигнали. Директивата (съображение 89 и член 20) предвижда, че държавите членки се насърчават да предоставят услуги за консултиране и социална подкрепа, предназначени да помогнат на хората да се справят с емоционалните и социалните предизвикателства, пред които могат да се изправят. Това е част от мерките за подкрепа и включва предлагане на достъп до психологическо консултиране, както и правни и финансови консултантски услуги за смекчаване на потенциалните професионални и икономически последици. Освен това мрежите за подкрепа, като групи от колеги/съмишленици или програми за наставничество, могат да помогнат на сигнализиращите лица да се справят с обществената реакция и да преодолеят чувството си на изолация. Кампаниите за повишаване на обществената информираност могат също така да играят роля за насърчаване на култура, която оценява подаването на сигнали, намаляване на стигмата и насърчаване на солидарността в общността и на работното място. Чрез прилагането на тези мерки държавите членки могат да създадат по-благоприятна среда, която не само защитава сигнализиращите лица, но и им дава възможност да действат в обществен интерес без страх от ответни мерки.

Финансова подкрепа

Само някои държави предлагат мерки за икономическа подкрепа в своята правна рамка, но тя е ограничена по обхват и размер. Сред тях Белгия и Словакия покриват разходите за частна правна помощ и разходите за частни здравни и/или психологически услуги.

Защита за подпомагащите лица

Директивата също така защитава лицата, които помагат на лицата, сигнализиращи за нередности, включително:

- помощници;
- членове на семейството;
- колеги.

Това гарантира, че те могат да помогнат на лицата, подаващи сигнали за нередности, без да се страхуват от отмъщение.

Свобода на печата и достъп до информация

Свободната преса играе решаваща роля за гарантиране, че лицата, подаващи сигнали за нередности, могат безопасно да споделят своите разкрития. Правителствата трябва да защитават независимостта на медиите, да защитават журналистите, отразяващи случаи на нередности, и да поддържат поверителността на източниците. Освен това достъпът до информация е от решаващо значение: лицата, сигнализиращи за нередности, се нуждаят от прозрачна правна рамка, която им позволява да подкрепят твърденията си с доказателства.

ОТВОРЕНО УПРАВЛЕНИЕ

Защита на лицата, сигнализиращи за нередности

Ефективната защита на лицата, сигнализиращи за нередности, би спечелила от координирани усилия между различни участници като институции, медийни организации, групи на гражданското общество, синдикати и органи за защита на правата на човека. Този подход на сътрудничество признава решаващата роля на сигнализиращите лица в различните сектори и засилва посланието, свързващо тяхното подаване на сигнали и защита с трудовите права и свободата на изразяване. Тази връзка е особено актуална в страни, в които се наблюдава нарастване на стратегическите съдебни дела срещу публично участие (SLAPP).

Специалисти от различни сектори посочват, че когато Директивата се прилага чрез създаването на нови специализирани органи или служби, отговарящи за подаването на сигнали за нередности, **многостранното участие може да бъде от решаващо значение за изграждането на доверие между всички участващи страни**, особено ако се осъществява в рамките на прилагането на Партньорство за отворено управление (OGP) в страната. Процеси като OGP предлагат полезна платформа за такъв диалог с множество заинтересовани страни. Конкретно това може да помогне за по-нататъшно задълбочаване на участието на представителите на частния сектор – независимо дали като отделни субекти или чрез представителни органи – и по този начин да допринесе за по-балансирана дискусия и по-ефективни механизми за защита.

Съдържателната ангажираност на заинтересованите страни следва да **обхване и участието в международни форуми като Конвенцията на ООН срещу корупцията (UNCAC)**. Това гарантира, че самите сигнализиращи лица, както и организациите, посветени на тяхната защита, участват активно в националните делегации и подготвителните дискусии. Силен пример за този подход беше видян на Десета сесия на Конференцията на държавите – страни по UNCAC (CoSP10) в Атланта през 2023 г.⁶⁹, където резолюцията относно защитата на сигнализиращите лица беше оглавена от бивш подател на сигнал, участващ в сръбската делегация. Това показва значението на включването на опита на служителите в процеса на изготвяне на политики, като се гарантира, че лицата, които са се сблъскали с ответни действия или са преминали през процеса на сигнализиране, допринасят за формирането на по-ефективна защита. **Чрез интегриране на сигнализиращите лица и групи за застъпничество в официални делегации, работни групи и преговорни процеси**, страните могат да разработят политики, които са не само добре информирани, но и практически и приложими. Този приобщаващ подход повишава легитимността, укрепва международното сътрудничество и гарантира, че рамките за защита на сигнализиращите лица се основават на реалните предизвикателства и нужди.

⁶⁹ Виж също: <https://whistleblowingnetwork.org/News-Events/News/News-Archive/Governments-Around-the-World-Step-Up-to-Support-Wh>

В допълнение към тези мерки за сътрудничество организациите на гражданското общество настоятелно препоръчват **широко тълкуване** на законите за защита на лицата, сигнализиращи за нередности, което надхвърля разпоредбите на Директивата и проправя пътя за бъдещата й реформа.

- Едно от ключовите предложения е да се разширят гаранциите за **организациите, които предоставят подкрепа и съвети на лицата, подаващи сигнали**, като се гарантира, че тези, които помагат на сигнализиращите лица, също са защитени от заплахи и отмъщение. Правителствата и гражданското общество могат да си сътрудничат за това разширяване, като признават решаващата роля, която тези организации играят за осигуряване на безопасно и ефективно оповестяване.
- Друга важна стъпка е постигането на **по-голяма хармонизация** между механизмите за защита на сигнализиращите лица и други правни рамки, като например тези, предназначени за **програми за защита на свидетели и сигнализиране във връзка с корупция, включваща организирани престъпни групи**. Един интегриран подход би помогнал да се гарантира, че лицата, които разкриват нарушения, получават адекватни мерки за сигурност.
- Въпреки че не са изрично обхванати от Директивата, организациите на гражданското общество се застъпват за разширяване на защитата, така че да се обхванат случаите, когато неправомерно поведение или корупция са разкрити **чрез достъп до обществена информация**. Това включва разкрития, направени от **журналисти, неправителствени организации, адвокати и активни граждани**, които в обществен интерес разкриват и съобщават за нередности.

Няколко международни инструмента подкрепят това по-широко тълкуване на защитата на лицата, сигнализиращи за нередности. Самата Директива 2019/1937/ЕС относно защитата на лицата, сигнализиращи за нередности, Европейският закон за свободата на медиите (EMFA) и Конвенцията на ООН срещу корупцията (UNCAC) със съответните резолюции допринасят за създаването на по-благоприятна правна среда за разширяване и хармонизиране на гаранциите. Чрез засилване на правната защита и разширяване на нейния обхват, правителствата могат да подобрят прозрачността, да насърчат отчетността и да създадат по-безопасни условия за тези, които говорят срещу нарушенията както в публичния, така и в частния сектор.

Подкрепа за подаване на сигнали

Положителна инициатива в контекста на „Отворено управление“ в подкрепа на лица, които биха подали сигнали за нередности, е създаването на **публичен регистър на организациите на гражданското общество, които предоставят безплатни услуги за подкрепа и съвети**, за да се подобри тяхното разпознаване и видимост. В Италия тази цел беше постигната чрез включване на този ангажимент в Петия национален план за действие за отворено управление (2021-2023 г.)⁷⁰. За тези, които желаят да повторят италианската инициатива, може да се препоръча:

- определяне на изискванията към организациите на гражданското общество да влязат в публичния списък, за да се гарантира безпристрастност, спазване на разпоредбите за неприкосновеност на личния живот и компетентност;
- насърчаване на разнообразен професионален опит в рамките на организациите на гражданското общество, за да се осигури цялостна подкрепа (правна, психологическа и др.);
- предвиждане на официални договорености с регистъра за подходящи организации на гражданското общество;
- поддържане на активна работна група сред членовете на регистъра за наблюдение на нуждите от обучение и информация и улесняване на партньорския обмен;
- провеждане на форуми най-малко два пъти годишно за справяне със системните предизвикателства, пред които са изправени организациите на гражданското общество, и опасенията, произтичащи от реални случаи, като същевременно се защита защитата на поверителността;
- насърчаване или изискване от всички публични органи да следват примера на регистъра, за да направят списъка видим и на своя уебсайт и в комуникацията със своите служители.

⁷⁰ Виж също: <https://www.opengovpartnership.org/members/italy/>

Друга, по-усъвършенствана мярка в рамките на отвореното управление е установяването на координация и работа в мрежа между признати консултантски и подкрепящи организации, за да се гарантира, че лицата, които биха подали сигнали за нередности, са насочени към най-подходящата организация за подкрепа. Например **може да се създаде единен център**, който да събира и оценява нуждите на лицата, сигнализиращи за нередности, след което да ги насочва към подходящата организация за подкрепа въз основа на териториален или специфичен за сектора експертен опит. Това ще помогне за рационализиране на процеса и ще гарантира, че хората получават най-ефективната помощ.

Такива услуги за правна и психологическа подкрепа следва да бъдат безплатни за лицата, които биха подали сигнали за нередности, за да се премахнат всички икономически пречки пред достъпа до услуги. За да гарантира това, правителството трябва да осигури **публично финансиране в подкрепа на институции и граждански организации**, както и **безплатна правна помощ** за лицата, подаващи сигнали за нередности, ако става въпрос за съдебни процеси.

4.7 ПРЕПОРЪКИ

За да се предложи цялостна подкрепа и защита на лицата, които имат достъп до процедури за подаване на сигнали, е от първостепенно значение да се насърчи ефективен и съвместен подход към подаването на сигнали. Това изисква участието на множество заинтересовани страни, всяка от които допринася със своя опит и роля за справяне с предизвикателствата, свързани с подаването на сигнали. Основните мерки за подобряване на подкрепата и защитата на лицата, сигнализиращи за нередности, включват:

1. ПОДОБРЯВАНЕ НА ДОСТЪПА ДО ПОДКРЕПА ЗА ЛИЦА, ПОДАВАЩИ ИНФОРМАЦИИ

Публичните и частните субекти следва да подобрят достъпността чрез публикуване на списъци на организациите на гражданското общество и други органи, които предлагат помощ и информация на лицата, сигнализиращи за нередности.

2. НАСЪРЧАВАНЕ НА НЕПРЕКЪСНАТО СЪТРУДНИЧЕСТВО

Непрекъснатото сътрудничество между компетентните органи, организациите на гражданското общество и други подходящи организации е от решаващо значение, за да се гарантира, че те са добре подготвени да предоставят висококачествени услуги на сигнализиращите лица.

3. ПОВИШАВАНЕ НА ОСВЕДОМЕНОСТТА И ИНИЦИАТИВИТЕ ЗА ОБУЧЕНИЕ

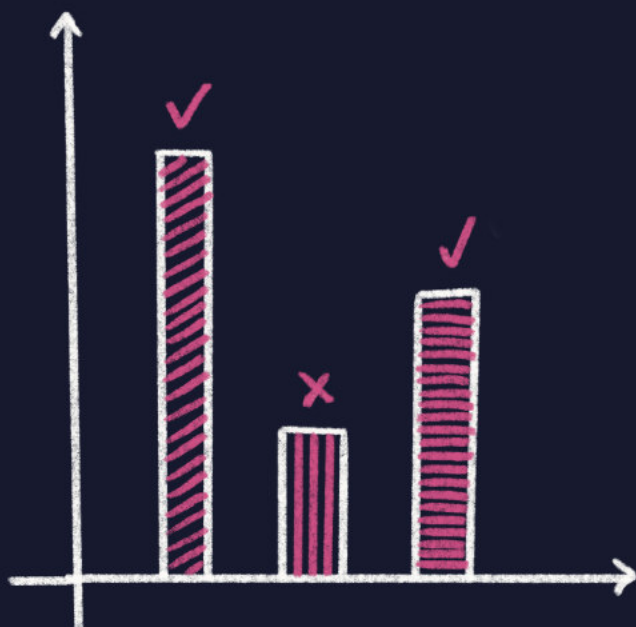
Администрациите и компаниите трябва активно да насърчават инициативи за повишаване на информираността и програми за обучение, за да подобрят разбирането на разпоредбите и процедурите за подаване на сигнали. Следва да се провеждат и целеви курсове за обучение на държавни служители за разработване на добри практики за разглеждане на сигнали и ефективно управление на свързаните с това процеси.

4. УЛЕСНЯВАНЕ НА ДИАЛОГА ЧРЕЗ СПЕЦИАЛНИ СРЕЩИ

На последно място, организирането на специални срещи с представители както на публичния, така и на частния сектор може да улесни конструктивния диалог, като позволи на заинтересованите страни да се справят с общите предизвикателства и съвместно да намерят оптимални решения.



Измерване и оценка на ефективността на системата и оценка на културата на подаване на сигнали за нередности



ГЛАВА 5

ИЗМЕРВАНЕ И ОЦЕНКА НА ЕФЕКТИВНОСТТА НА СИСТЕМАТА И ОЦЕНКА НА КУЛТУРАТА НА ПОДАВАНЕ НА СИГНАЛИ ЗА НЕРЕДНОСТИ

ГЛАВА 5

5.1 ИЗМЕРВАНЕ НА ВАЖНОТО: ЕФЕКТИВНОСТ, ИНФОРМИРАНост И КУЛТУРНИ АСПЕКТИ

Ефективните системи за подаване на сигнали за нередности допринасят за **засилване на прозрачността и отчетността** в ЕС. За да се гарантира тяхното положително въздействие, ефективността на тези системи, заедно с нивото на информираност и разбиране на процеса на подаване на сигнали, следва редовно да се измерват и оценяват. С Директивата, въпреки предизвикателства като забавеното ѝ транспониране в повечето държави членки, непълното ѝ интегриране в националните правни системи и очевидната сложност на рамката, вниманието се измества към оценката на ефективността на тези системи и културните фактори, които влияят върху техния успех.

В **България**, както беше посочено, има известно объркване и служителите понякога изпитват затруднения да разберат обхвата на Директивата, особено когато става въпрос за трудови права или нарушения, които могат да изглеждат по-скоро лични, отколкото да засягат по-широк обществен интерес. Един от интервюираните експерти в **Италия** признава, че в новото законодателство за защита на сигнализиращите лица има положителни нововъведения, но подчертава редица критични въпроси, като например проблема с координацията в случай на оповестяване чрез социалните медии. Според един от интервюираните експерти от **Испания** прилагането на закона е трябвало да бъде придружено от процесуални реформи, включително засилване на мерките за защита.

Последните събития подчертават необходимостта от оценка на системите за подаване на сигнали за нарушения не само като инструменти за съответствие, но и като **неразделни механизми** за насърчаване на етичното поведение и организационната почтеност. Съвременните изследвания и практика подчертават необходимостта от

всеобхватни методи за оценка, за да се гарантира, че каналите за подаване на сигнали са достъпни, надеждни и ефективни за справяне с нарушенията, като същевременно защитават сигнализиращите лица от ответни действия. Освен това културното измерение, обхващащо доверието, информираността и готовността на служителите да сигнализират, се очертава като крайъгълен камък в създаването на **проактивна култура на открито говорене**.

5.2 ПРЕГЛЕД НА СЪЩЕСТВУВАЩИТЕ ИНСТРУМЕНТИ ЗА ИЗМЕРВАНЕ И ОЦЕНКА

5.2.1 Международна организация по стандартизация

Рамката ISO 37002:2021 служи като аналитичен инструмент за създаване на политики и предлага информация за прилагането на системи за управление на сигнали за нередности (WMS) в различни институции⁷¹. Тя предоставя насоки за създаване, прилагане и поддържане на ефективна WMS, основана на принципите на доверие, безпристрастност и защита. Рамката включва четири ключови стъпки:

- получаване на сигнали за нарушения,
- оценка на получените сигнали,
- разглеждане на получените сигнали, и
- приключване на случаите по подадените сигнали.

Замислени да бъдат универсално приложими, тези насоки са подходящи за организации от всякакъв размер, вид и сектори, включително публични, частни и нестопански субекти.

Рамката предоставя стандартизиран подход за оценка на системите за подаване на сигнали за нередности с цел да се улесни изготвянето на политиките и подобренията в управлението. Проучванията на редица случаи подчертават, че прилагането на този стандарт за системите за управление на сигналите за нередности често е частично и изисква по-нататъшно развитие в конкретни области, като например политиките за информираност и защита на сигнализиращите лица. Така че може в някои случаи да се наложи рамката да бъде адаптирана, за да отговори на специфичните организационни нужди.

5.2.2 Цифрови платформи за сигнализиране

Законодателният акт за цифровите услуги⁷² въвежда инструменти за създаване на по-безопасно, по-справедливо и по-прозрачно онлайн пространство в ЕС⁷³. Сред тях е инструментът за подаване на сигнали за

⁷¹ International Organisation for Standardization, ISO 37002:2021. Whistleblowing management systems – Guidelines [Международна организация по стандартизация, ISO 37002:2021. Системи за управление на подаването на сигнали за нередности – насоки], <https://www.iso.org/obp/ui/en/#iso:std:65035:en>

⁷² Регламент (ЕС) 2022/2065 на Европейския парламент и на Съвета от 19 октомври 2022 г. относно единния пазар на цифрови услуги и за изменение на Директива 2000/31/ЕО (Акт за цифровите услуги), <https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32022R2065>

⁷³ Европейска комисия. Digital Services Act whistleblower tool: Report inside information about online platforms, [Европейска комисия. Инструмент за подаване на сигнали за цифрови услуги: Докладвайте вътрешна информация за онлайн платформи], <https://digital-services-act-whistleblower.integrityline.app>

цифрови услуги, който позволява да се идентифицират вредни практики на много големи онлайн платформи и онлайн търсачки (VLOP/VLOSE)⁷⁴. Той осигурява сигурен и по избор анонимен канал за докладване на вътрешна информация (като например доклади, бележки, обмен на електронни съобщения, показатели за данни, вътрешни проучвания, решения и други съответни обстоятелства, независимо дали са минали, настоящи или бъдещи). Обхватът на сигнализирането обаче е ограничен до практики, които нарушават задълженията за цифровите услуги, като например модерирание на съдържание, функциониране на препоръчани системи, реклама, оценка и смекчаване на рисковете, свързани с основните права на потребителите, обществената безопасност и здравеопазването, гражданските дискусии, изборните процеси и правата на децата. Въпреки че цифровите платформи подобряват достъпността и ефективността на сигнализирането, те предлагат ограничени възможности за сигнализиране по тесен кръг от въпроси. Освен това тяхното използване и ефективност зависят до голяма степен от приемането и доверието на потребителите в системата.

5.2.3 Емпирични проучвания: опитът на Полша и Италия

През декември 2022 г. е проведено емпирично проучване сред специалисти по човешки ресурси, мениджъри и директори в Полша, преди полският Закон за лицата, сигнализиращи за нередности, да влезе в сила на 25 септември 2024 г. Проучването се фокусира върху подаването на сигнали за нередности в по-широкия контекст на риска за персонала, като изследва нагласите на ръководителите към риска, източниците на риск за персонала, ефективността на системите за съответствие в областта на човешките ресурси (включително механизмите за подаване на сигнали), както и поведението и загубите, свързани с рисковете, произтичащи от човешкия фактор. Събирането на данни използва както компютърно подпомагано интервюиране по интернет (CAWI), така и компютърно подпомагано интервюиране по телефона (CATI). Приложени са статистически анализи, включително хи-квадратна проверка (chi-squared test)⁷⁵ с корекция на Йейтс и тестът на Крускал-Уолис, за да се анализират разликите в оценките на процесите на подаване на сигнали въз основа на променливи като длъжност, размер на компанията, форма на собственост и индустриален сектор⁷⁶.

Основните резултати от **ПОЛСКОТО** проучване са:

- Подаването на сигнали за нередности е широко приет важен инструмент както за разкриване на нарушения в организациите, така и за ефективно управление на съответствието⁷⁷.
- Една трета от респондентите не са изразили ясно становище относно ефективността на утвърдените системи за подаване на

⁷⁴ Европейска комисия. *Supervision of the designated very large online platforms and search engines under DSA*, [Европейска комисия. Надзор на определените много големи онлайн платформи и търсачки съгласно законодателните актове за цифровите услуги], <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses#ecl-inpage-lqfbha7vv>

⁷⁵ Хи-квадратната проверка е тест за статистически хипотези, използван при анализа на контингентни таблици, когато размерът на извадките е голям (бел. ред.).

⁷⁶ Winnicka-Wejs, A. "Whistleblowing as a tool for HR compliance management system – survey report". *Scientific Papers of Silesian University of Technology 2023. Organisation and Management Series no. 182*, 2023, pp. 573-596. DOI , 10.29119/1641-3466.2023.182.34 <https://managementpapers.polsl.pl/wp-content/uploads/2023/12/182-Winnicka-Wejs.pdf>

⁷⁷ Пак там.

сигнали за нередности.

- Респондентите в компании със среден размер са дали по-високи оценки на вътрешните канали за подаване на сигнали за нередности и за защита срещу ответни мерки с цел отмъщение в сравнение с други организации. Разликите в оценките въз основа на длъжността могат да се дължат на различията в организационната култура, доверието на служителите в ефективността на системите за подаване на сигнали, обхвата на подлежащите на сигнализиране нарушения и адекватността на вътрешните канали.
- Като цяло професионалистите оценяват системите за подаване на сигнали в своите организации по-ниско от останалите. Специалистите по човешки ресурси, мениджърите и директорите по човешки ресурси не са единодушни в оценката си за съществуващото ниво на доверие на служителите в правилното функциониране и надеждността на системите за подаване на сигнали в техните организации⁷⁸.

Паралелно емпирично проучване е проведено в **Италия** от Националното училище по администрация (SNA) в рамките на проект „Обучение за промяна. Отворена администрация и иновативни модели на обучение за ефективно прилагане на подаването на сигнали за нередности“⁷⁹. Целта му е да се оцени въздействието на програмите за обучение на SNA върху възприемането на подаването на сигнали за нередности, като се има предвид относително слабото му утвърждаване в италианската правна и организационна култура.

Италианското проучване използва методология, подобна на полското проучване, като се основава на техниките CAWI и CATI. Данните са събрани от извадка от специалисти по човешки ресурси, мениджъри и държавни служители, като са приложени статистически анализи като хи-квадратна проверка с корекцията на Йейтс и теста на Крускал-Уолис, за да се изследват разликите въз основа на длъжността, организационната структура и сектора.

Основните резултати от **италианското** проучване са:

- Обучението играе решаваща роля не само за разпространението на информираността и знанията за подаването на сигнали, но и за трансформирането на общественото възприятие за него.
- Доверието и културните бариери остават големи предизвикателства въпреки правната защита.
- Подкрепящата роля на организациите на гражданското общество е недостатъчно използвана и не е добре известна (преди обучението само 13% от анкетираните са били наясно с ролята си, след обучението процентът нараства до 46,6%).
- Вътрешните канали са по-малко предпочитани (38% от анкетираните), повече са предпочитанията за външното сигнализиране (61%), тъй като то се счита за по-надеждно, независимо и ефективно.

⁷⁸ Пак там.

⁷⁹ Donini, V. M., Lostorto, V., & Zamaro, N. (2022). *Formare per trasformare: l'impatto trasformativo della formazione sulla prevenzione della corruzione. Prime riflessioni*. Rivista di diritto amministrativo – Amministrativamente, 4(2022), <https://www.amministrativamente.com/index.php/formez/article/view/13339>

- Основните стимули за докладване на нарушения са: защита от отмъщение (74,2% от жените, 67,9% от мъжете), гаранции за поверителност (68,5% от жените, 67% от мъжете), увереност, че сигналът ще бъде разгледан (59,2% от жените, 57,8% от мъжете) и убеденост, че повдигнатият въпрос е важен/сериозен (41,7% от жените, 46,4% от мъжете).
- Паричната награда не се приема за значим стимул (само 3,8% от жените, 7,3% от мъжете).
- Проучването подчертава необходимостта от допълнително обучение за повишаване на информираността, насърчаване на сигнализирането за нередности като етично задължение и подобряване на защитата за изграждане на доверие в системата.

Освен това, по отношение на **Италия** е интересно да се отбележи, че Националният орган за борба с корупцията (ANAC) е изпратил въпросник до субектите от публичния и частния сектор, насочен към проверка на решенията, приети във фазата на първоначалното прилагане на законодателството. В публичния сектор 62% от субектите са създали технологична платформа, специално предназначена за получаване и обработване на сигнали в писмена форма, а 38% не са създали такава платформа и са възприели различни методи за получаване на сигнали, като например сертифицирана електронна поща или обикновена поща.

В това отношение трябва да се подчертаят два критични аспекта:

- сред субектите, които не са създали платформа, има и големи администрации, които разполагат с всички инструменти по отношение на наличието на човешки и материални ресурси за лесно изграждане на технологичната инфраструктура;
- сертифицираната електронна поща и обикновената поща не представляват подходящи методи за получаване на сигнали, ако не се съпътстват от конкретни мерки за сигурност, насочени към намаляване на риска от неправомерно разкриване на данни.

Същите критични резултати, очертани по-горе, са регистрирани и в частния сектор: само 56% от участниците в проучването имат работеща технологична платформа, а приблизително 64% заявяват, че са предвидили възможност за подаване на устни сигнали. Освен това в частния сектор само 30% от субектите декларират, че са получавали сигнали за нередности: това е знак, че рамката за подаване на сигнали за нарушения все още е малко известна и трябва да бъде допълнително насърчавана.

Както полското, така и италианското проучване показват, че въпреки признаването на важността на сигнализирането, служителите често не вярват в ефективността на механизмите за подаване на сигнали и се страхуват от ответни действия. Въпреки че инициативите за обучение, както се вижда от италианското проучване, спомагат за подобряване на информираността, културните бариери и институционалните слабости продължават да възпрепятстват създаването на стабилна култура на подаване на сигнали. Справянето с тези предизвикателства изисква не само правна рамка, но и проактивни организационни политики, по-

ясна комуникация и засилена защита за насърчаване на култура на почитеност и прозрачност. Макар резултатите от проучванията да не са представителни и да не могат да бъдат обобщени на национално ниво, те могат да бъдат полезни за собствениците на компании, мениджърите, специалистите по човешки ресурси и служителите по съответствието, които са ключови заинтересовани страни, отговорни за прилагането на ефективни системи за подаване на сигнали на работното място.

5.3 ИНДЕКС ЗА ОЦЕНКА НА ЗАЩИТАТА НА ЛИЦАТА, СИГНАЛИЗИРАЩИ ЗА НЕРЕДНОСТИ

Индексът за оценка на защитата на лицата, подаващи сигнали за нередности, разработен от група изследователи, е цифров инструмент за оценка на **ефективността на механизмите за защита** в различни държави и периоди от време.

Индексът се състои от количествени и качествени подиндекси. **Първите оценяват** институционалните гаранции чрез показатели като сигурност на работното място, поверителност, защита от ответни действия с цел отмъщение, съдебен имунитет, нива на защита на сигнализиращите лица (брой искания за защита в сравнение с общия брой сигнали) и др. **Вторите са насочени към улавяне** на възприятията и преживяванията, свързани с подаването на сигнали, включително възприятията (на различни групи като длъжностни лица, експерти, граждани без опит в подаването на сигнали и самите сигнализиращи лица) и опита (само на сигнализиращите лица).

Индексът позволява сравняване на нивата на защита на лицата, сигнализиращи за нередности, в различните държави, както и проследяване на промени във времето. Освен измерването, той очертава ключови области на подобрене, като навременно прилагане на законите, безпристрастност при назначаването на длъжностни лица и **прозрачност на наличните данни**.

Авторите се застъпват за методология от два стълба, комбинираща административни данни с резултати от проучвания, и подчертават необходимостта от стандартизиране и подобряване на достъпа до съответните данни.

5.3.1 Асоциация „Прозрачност без граници“

След публикуването на методология за оценка на съответствието на проектите на закони с Директивата на ЕС за защита на лицата, сигнализиращи за нередности, и добри практики⁸⁰, Асоциация „Прозрачност без граници“ разработва рамка за самооценка, за да помогне на организациите да създават, прилагат и преразглеждат вътрешни системи за сигнализиране, които са ефективни и в

⁸⁰ Transparency International. Assessing Whistleblowing Legislation: Methodology and Guidelines for Assessment Against the EU Directive and Best Practice. 23 September 2020, <https://www.transparency.org/en/publications/assessing-whistleblowing-legislation>

съответствие с най-добрите практики и международните стандарти⁸¹. Рамката включва 130 въпроса, обхващащи осем измерения, вариращи от обхвата на системата и защитата, която тя предоставя, до комуникацията в и за системата, и мониторинга на нейната ефективност⁸². Въпросите са предназначени да идентифицират потенциални фактори, които биха могли да подкопаят вътрешните системи за сигнализиране. Отговорите и констатациите могат да помогнат на организациите да подобрят ефективността на своите вътрешни системи в съответствие с най-добрите практики и международните стандарти.

5.4 ОСНОВНИ ПОКАЗАТЕЛИ ЗА ОЦЕНКА НА СИСТЕМИТЕ ЗА ПОДАВАНЕ НА СИГНАЛИ ЗА НЕРЕДНОСТИ

Въз основа на съществуващите инструменти и като взема предвид състоянието и нуждите на системите за защита на лицата, сигнализиращи за нередности в рамките на ЕС и държавите членки, настоящият раздел има за цел да формулира **набор от количествени и качествени показатели**, които могат да се използват за оценка на ефективността на механизмите за подаване на сигнали за нередности.

От количествена гледна точка ключовите показатели за оценка са свързани главно с функционирането на механизмите за сигнализиране. Те трябва да включват, наред с другото:

- получени сигнали и основателни сигнали: общият брой на получените сигнали за нередности и делът на тези, които са приети за основателни след разследване, за определен период (напр. годишно);
- разследвания и резултатите от тях: брой извършени разследвания и резултатите от тях;
- време за отговор/решаване: средното време, необходимо за потвърждаване, разследване и решаване на проблемите, свързани с подадените сигнали;
- достъпност на каналите за сигнализиране: наличие на основани на пола, разнообразни и лесни за използване канали (напр. онлайн формуляри, горещи линии, възможности за срещи лице в лице), тяхната използваемост сред различните демографски групи и зачитане на равенството между половете;
- съдебни производства и съдебни решения: броят на образуваните съдебни производства, включително производствата за прекратяване на ответни действия, и постановените съдебни решения, за определен период от време (напр. годишно);
- случаи на ответни действия с цел отмъщение и защитни мерки: броят на лицата, сигнализиращи за нередности, които са били подложени на ответни действия с цел отмъщение, и мерките, предприети за справяне с такива случаи (ефективност на защитата);
- анонимност и поверителност: наличието на мерки за защита на

⁸¹ Transparency International. Internal Whistleblowing System Self-assessment Framework, <https://forms.office.com/Pages/ResponsePage.aspx?id=d2r57HSK7U-hwgM32S0wX1aBYjEGkwIJtPtUD4e4zFIUM0pCTTkwQVVKWFRIN1kyTzU3UFVRRREIMNy4u>

⁸² Transparency International. Internal whistleblowing systems: self-assessment framework for public and private organisations, 31 October, 2024, <https://www.transparency.org/en/publications/internal-whistleblowing-systems-self-assessment-framework-public-private-organisations>

сигнализиращите лица и гарантиране на анонимност;

- последващи действия: делът (процентът) на случаите, довели до коригиращи действия или промени в политиките/правилата;
- финансови глоби и възстановени суми: суми, събрани от наложени глоби и други наложени финансови санкции;
- оценка на финансовите щети: оценка на финансовите загуби, свързани с подадените сигнали.

Предложените показатели предоставят измерима информация за ефективността на системата. Методите за събиране на данни за тези показатели могат да включват:

- проучвания и въпросници, разпространени сред служителите и заинтересованите страни, за измерване на информираността, доверието и възприемането на системите за сигнализиране;
- анализ на статистическите данни за сигналите, процентите на разрешените случаи и резултатите от защитата, съдебната статистика и свързаните с нея показатели (анализ на данни);
- оценка на съответствието със законодателството и насоките за подаване на сигнали за нередности, вътрешните правила и политики (одити за съответствие).

В страни като **България**, където на настоящия етап измерването на ефективността на системата за подаване на сигнали е трудно поради малкия брой сигнали и съдебни дела, фокусът трябва да се измести към изграждане на доверие чрез положителен опит и прозрачност. Бързите действия след сигнала и осигуряването на поверителност са от ключово значение за изграждането на доверие в системата и насърчаването на повече служители да я използват. Ако работниците/служителите видят, че сигналите водят до реални резултати и че самоличността на лицата, подаващи сигнали за нередности, се пази в тайна, те ще бъдат по-мотивирани да участват.

Що се отнася до качествената обратна връзка, акцентът следва да бъде поставен върху непреки или анонимни подходи, като например обобщени проучвания, документни проучвания или сигурни канали за обратна връзка, които гарантират поверителността и защитата на лицата, сигнализиращи за нередности. Те включват:

- фокус групи, проведени отделно с работници/служители и лица, подаващи сигнали за нередности, за да се проучат опита със системата и културните нагласи към сигнализирането;
- проучвания на конкретни случаи:
 - анализ на рамката за защита на лицата, сигнализиращи за нередности, включително съответствието ѝ с Директивата на ЕС, националното законодателство, вътрешните правила и процедури (спазване на законодателството), както и наличието на психологическа подкрепа, правна помощ и други мерки за сигнализиращите лица (механизми за подкрепа);
 - анализ на конкретни сигнали за нередности за оценка на обработката и резултатите от процеса;
 - анализ на финансовите постъпления от глоби и санкции и оценка

на установените финансови щети.

- интервюта със заинтересованите страни, като например организации на гражданското общество, професионални асоциации, синдикати и регулаторни органи, за да се проучи сътрудничеството и системното въздействие.

За да се насърчи подаването на сигнали за нередности и да се подобрят системите за сигнализиране, могат да се препоръчат допълнителни инструменти, като например:

- публикуване на подробни оценки на ефективността на системите за подаване на сигнали и културата на подаване на сигнали;
- събиране на редовна обратна връзка от лица, подаващи сигнали за нередности, служители и заинтересовани страни за идентифициране на пропуски;
- използване на резултатите от оценката за усъвършенстване на механизмите за сигнализиране, програмите за обучение и рамките за защита.

5.5 ОЦЕНКА НА КУЛТУРАТА НА ОТКРИТО ГОВОРЕНЕ

Утвърдената култура на открито говорене е от съществено значение за успеха на системите за подаване на сигнали.

В този смисъл са важни методите за оценка на доверието на служителите в каналите за сигнализиране, желанието им да подават сигнали за нарушения и тяхното възприятие за отзивчивостта на ръководството. На различни равнища на ЕС поверителността, включително защитата на самоличността на лицата, сигнализиращи за нередности, се признава за основен и ефективен начин за насърчаване на служителите да съобщават за проблеми⁸³.

Набор от инструменти за оценка на информираността на служителите, доверието им в системата за подаване на сигнали, честотата на сигнализиране и т.н., могат да се използват за оценка на ангажираността в културата на открито говорене:

- делът на служителите, които са запознати с механизмите за подаване на сигнали и за правата си като сигнализиращи лица може да се използва за оценка на информираността на служителите;
- проучвания за измерване на доверието на служителите в реакцията на организацията на сигнали за нередности;
- заявено желание и способност на служителите да сигнализират.

Инструменти като проучвания и фокус групи също могат да се използват за идентифициране на бариери пред откритото говорене и за подкрепа на стратегии за създаване на отворена и подкрепяща среда за лицата, подаващи сигнали за нередности:

⁸³ European Data Protection Supervisor (EDPS). Guidelines on processing personal information within a whistleblowing procedure, December 2019, https://www.edps.europa.eu/sites/default/files/publication/19-12-17_whistleblowing_guidelines_en.pdf?utm_source=chatgpt.com

- проучвания или интервюта с мениджъри за техните възприятия за подаване на сигнали и откритост на сигнализирането могат да предоставят информация за нагласите на ръководството;
- доверието на външните заинтересовани страни в ангажимента на организацията за защита на лицата, сигнализиращи за нередности, е показател за обществено доверие;
- обратната връзка от лицата, подаващи сигнали за нередности, относно справедливостта и прозрачността на разследванията е важен показател за степента на удовлетвореност от разрешаването на сигнализираните проблеми.

За да се гарантира широка информираност, е от съществено значение да се повиши обществената осведоменост: например заинтересовани страни от **Италия** разкриват интересни идеи по тази тема. За да се разпространи културата на подаване на сигнали в обществото, посланието за подаване на сигнали трябва да бъде предадено чрез средства, които могат да достигнат до по-широка аудитория. За да се насърчи културата на подаване на сигнали, се предполага, че Лига Серия А може да използва голямата си неделна аудитория, за да стартира кампания за повишаване на информираността и „да действа като говорител по такъв чувствителен въпрос, както е правила по други въпроси като дискриминация, злоупотреби, убийства на жени и т.н.“. Друго предложение е да се разработят ключови елементи на комуникацията за оценка на общественото възприятие за подаване на сигнали, като например: култура на открито говорене, общностна журналистика, журналистика на решенията, обществени услуги и колективни проблеми. За други идеята за подаване на сигнали за нередности трябва да се разглежда като демократична свобода, една от проявите на демокрацията, която трябва да се защитава заедно със свободата на изразяване. Освен това определението за подаване на сигнали като форма на свобода на изразяване на мнение се счита за важно нововъведение в правната рамка за подаването на сигнали за нередности. Предлага се и интересен подход за противодействие на културата на мълчание и установяване на нова етика – повишаване на отговорността на гражданите, утвърждаване на съзнанието, че сигнализирането за нередности е личен избор, засилване на разбирането, че сигнализиращият е обикновен човек, който прави обикновени неща. Освен това се подчертава, че следва да се създаде култура, която да прави системата все по-малко институционална, например чрез овластяване на гражданите да поемат отговорност, тъй като културата на безотговорност може да доведе до наплив от клеветнически или неверни сигнали, подадени с цел лична изгода, които претоварват системите за сигнализиране.

Заинтересованите страни в **Испания** подчертават необходимостта от промяна на културата и начина на мислене в посока, че лицата, подаващи сигнали за нередности, не са информатори, а сътрудници, така че сигнализиращите за нередности да се разглеждат като интелигентен източник на информация и да се покаже на лицата, които биха подали сигнали, че сигнализирането не е безполезно и че е необходимо да се изгради доверие в процеса.

В **Испания** е широко разпространена културата на мълчание, продиктувана от страх от отмъщение и изключване, което се наблюдава на работното място подобно на децата в училище, където всяко дете, което сигнализира за неподходящо поведение, се възприема като доносник.

В **България** културата на подаване на сигнали за нередности изглежда недостатъчно развита и служителите имат малък интерес или увереност в използването на системата. Интервюираните споделят разбирането, че културата на подаване на сигнали трябва да бъде подкрепена от механизми за доверие с редовна оценка на ефективността на системата. Интервюираните заявяват, че повишаването на доверието и ефективността на системата изисква непрекъсната обратна връзка, мониторинг и коригиране на процедурите. Предложенията включват извършване на редовни прегледи на вътрешните политики и споделяне на опит с други организации за подобряване на цялостната култура на подаване на сигнали.

Според практикуващи юристи в **България** трябва да се установи ясна връзка, както законодателна, така и в практиката, а и в общественото разбиране, между защитата на свободата на словото в стратегическите съдебни дела срещу публично участие (SLAPP) и защитата на лицата, подаващи сигнали за нередности. Засега това разбиране не е видимо в правото на ЕС, националното право, съдебната практика и общественото разбиране. Практикуващите юристи се опитват да свържат концепцията за SLAPP и законодателството за защита на лицата, сигнализиращи за нередности, например чрез защитата по дела за клевета. Въпреки че някои съдилища проявяват интерес към този подход, резултатите остават несигурни поради липсата на установена съдебна практика. Очаква се обаче резултатите по някои от тези случаи скоро да станат ясни.

Проучването на възприятията и равнището на приемането от страна на заинтересованите страни може да даде важна информация за състоянието на културата на открито говорене и да помогне за трансформирането на културата на мълчание в култура на активно подаване на сигнали.

5.6 ОЦЕНКА НА АНГАЖИРАНОСТТА И СЪТРУДНИЧЕСТВОТО НА ЗАИНТЕРЕСОВАНИТЕ СТРАНИ

Заинтересованите страни играят решаваща роля за успеха на инициативите за подаване на сигнали за нередности – от подпомагане на политиките до предприемане на действия по сигнализираните проблеми. Поради това е важно да се използват подходящи методи за оценка на ефективността на сътрудничеството между заинтересованите страни, като фокусът се постави върху комуникацията, съгласуването на политиките за подаване на сигнали и съвместните усилия за повишаване на информираността. Набор от показатели може да се използва за измерване на сътрудничеството между заинтересованите страни.

Предложените показатели могат да измерват:

- интензитет на ангажираността: брой съвместни обучения, кампании за повишаване на осведомеността или форуми с други заинтересовани страни;
- споделени ресурси: съществуване и използване на партньорства за споделени ресурси (напр. правна помощ, инструменти за разследване);
- съвместно разработване на политики: включване на заинтересованите страни в разработването на политики или насоки за лицата, сигнализиращи за нередности.

Редица методи могат да се използват за оценка на ангажираността и сътрудничеството на заинтересованите страни в инициативи за подаване на сигнали за нередности, включително:

- съвместни проучвания за оценка на удовлетвореността на заинтересованите страни от съвместни инициативи, даващи представа за техните възприятия за ефективност и области за подобрене;
- мрежови анализ за картографиране на потока от информация и ресурси между заинтересованите страни и идентифициране на силните страни и пропуските в комуникацията и споделянето на ресурси;
- анализ на резултатите за измерване на осезаемото въздействие на съвместните усилия, като например, увеличаване на сигналите за нередности или решените случаи.

ОТВОРЕНО УПРАВЛЕНИЕ

Редовното събиране на данни и анализът на дейностите, свързани с подаването на сигнали за нередности, са от ключово значение за оценката на ефективността на системата. Показатели като посочените в настоящата глава в крайна сметка следва да послужат за основа за промени в политиката. Принципите на отвореното управление предполагат, че:

- данните винаги се публикуват по **стандарты за отворени данни**;
- събирането и прозрачността на данните включват информация за **процедурите на политиката и процесите на ангажиране на заинтересованите страни**;
- констатациите се съобщават прозрачно и се обсъждат със заинтересованите страни, като се гарантира, че **заклученията водят до практически подобрения**, които могат да бъдат разработени съвместно в рамките на ангажимент по Националния план за действие или като самостоятелно предизвикателство за отворено управление, което позволява амбициозни ангажименти за реформи да бъдат поети и признати извън редовния цикъл на плана за действие.

В обобщение, за да се подобрят и направят по-прозрачни редовните оценки на ефективността на системите за подаване на сигнали за нередности, културата на открито говорене и ангажираността на заинтересованите страни, се препоръчват следните минимални изисквания:

- редовно публикуване, поне веднъж годишно, на подробни оценки на ефективността на системата за подаване на сигнали и културата на подаване на сигнали;
- редовно събиране на обратна връзка от лица, подаващи сигнали за нередности, служители и заинтересовани страни за идентифициране на пропуски и области за подобрене;
- използване на резултатите от оценката за усъвършенстване на механизмите за сигнализиране, програмите за обучение и рамките за защита.

В заключение, въпреки че правната рамка за подаване на сигнали за нередности е налице на европейско и национално равнище, често липсва необходимата инфраструктура и практически мерки за ефективното ѝ прилагане. Принципът на отворено управление изисква създаването на институционален механизъм, или нова институция, или съществуваща, която да подкрепя пълното, справедливо и отговорно прилагане на законодателството за подаване на сигнали за нередности, да помага на хората в трудни ситуации, да намира разумни решения и като цяло да допринася за подобряването както на законодателството, така и на системите за подаване на сигнали.

5.7 ПРЕПОРЪКИ

Какво може да се препоръча въз основа на емпиричните изследвания?

1. ПРОВЕЖДАНЕ НА РЕДОВНИ ЕМПИРИЧНИ ИЗСЛЕДВАНИЯ

Като се вземе предвид емпиричното проучване, проведено в Полша (2.3), може да се препоръча подобни проучвания да се провеждат редовно в държавите членки, за да се съберат съответните данни и да се изгради теоретична и емпирична основа относно възприемането и ефективността на системите за подаване на сигнали за нередности в различен организационен и национален контекст. Това ще даде възможност за наблюдение на развитието на системите и непрекъснато подобряване на тяхната ефективност.

2. АДАПТИРАНЕ НА ИНДЕКСА ЗА ОЦЕНКА НА ЗАЩИТАТА НА ЛИЦАТА, ПОДАВАЩИ СЪОБЩЕНИЯ (IEWP)

Индексът за оценка на защитата на лицата, сигнализиращи за нередности (2.4) може да бъде взет предвид и адаптиран от държавите членки при разработването на техни собствени показатели за оценка. Въпреки че индексът се основава на изследвания в публичния сектор, той може да бъде адаптиран за проследяване и оценка на сигнализирането за нередности в частния и нестопанския сектор, като по този начин ефективно се обхванат всички форми на корупция и институционални злоупотреби.

3. ИЗПЪЛНЕНИЕ НА КЛЮЧОВИ ПРЕПОРЪКИ НА ТИ КЪМ СИСТЕМИТЕ ЗА ПОДАВАНЕ НА СИГНАЛИ

При създаването и поддържането на вътрешна система за подаване на сигнали трябва да се вземат предвид някои ключови препоръки от Асоциация „Прозрачност без граници“ (2.5). Те включват гарантиране, че системата отговаря на националните правни изисквания (закони за защита на лицата, сигнализиращи за нередности, и други относими закони, като например законодателството за защита на данните или трудовото законодателство), че е приобщаваща и чувствителна към аспектите на пола, че се преразглежда официално поне веднъж годишно и че се правят подходящи промени за подобряване на нейната ефективност.

РАВЕНСТВО МЕЖДУ ПОЛОВЕТЕ

Редовното събиране на данни и анализ на дейностите по подаване на сигнали за нередности са от ключово значение за оценката на ефективността на системата. Въпреки че жените са склонни да осъждат корупционното поведение повече от мъжете, **те изглежда съобщават за корупция по-рядко от мъжете**, както се потвърждава от данните на Глобалния барометър на корупцията (GCB) на Асоциация „Прозрачност без граници“⁸⁴.

Някои **ключови констатации** от различни изследвания:

- Само **48% от жените вярват, че могат да сигнализират за случаи на корупция без риск** от отмъщение, в сравнение с 54% от мъжете⁸⁵.
- **Стимули за сигнализиране:** експериментално проучване сред над 2 000⁸⁶ служители показва, че жените имат по-голям стимул от мъжете да предприемат действия, ако има **защита срещу отмъщение и законово задължение**.
- Според проучване в Италия⁸⁷ няма съществена разлика в желанието за сигнализиране между мъжете и жените. Това, което трябва да бъде допълнително проучено обаче, е **страхът от отмъщение от страна на мениджъри и колеги и повишените нива на стрес**, който жените изпитват след подаване на сигнал.

Като цяло изглежда, че сред експертите, интервюирани за целите на това ръководство, има тенденция да не се вземат предвид трудностите и сложността на **„откритото говорене“** при жените, а по-общо при всички маргинализирани група. Ако обаче данните показват, че жените са склонни да говорят по-малко и да страдат повече от страха от отмъщение, това **трябва да служи като индикатор** за ефективността на системата.

Препоръчва се:

- **приоритизиране на темата за жените, които страдат повече** от мъжете от вреди и отмъщение;
- **повишаване на осведомеността за необходимостта от приобщаващ подход** към всички различия и по-слаби групи, които могат да присъстват в организационната култура;
- **повишаване на осведомеността относно случаите** на сексуално изнудване и сексуален тормоз (за допълнителна информация по тази тема вижте карето в **Глава 1**);
- публикуване на данни, разбити **по пол**, когато има такива: само малко на брой организации събират данни за пола и други междусекторни фактори. Това е **пропуснатата възможност** за събиране на актуална информация, която би могла да подпомогне **вземането на решения, основани на факти**; за справяне с този проблем е от съществено значение да се засилят механизмите за събиране и анализ на данни, като се гарантира по-точно разбиране на поведението, нуждите и приоритетите на лицата, подаващи сигнали за нередности.
- **обучение и повишаване на осведомеността относно подаването на сигнали за нередности, чувствително към особеностите на пола;**
- **разработване на програма за обучение в рамките на организацията като превантивна мярка**, насочена към обучение на всички членове и участници в практиките за подаване на сигнали за нередности, с фокус върху пола и пресечната точка на други фактори на уязвимост, като бедност и дисбаланс на силите. Програмата следва да разглежда сигнализирането за тормоз, сексуално насилие и свързани с корупция неправомерни действия, като същевременно подчертава различното въздействие върху жените и мъжете, особено непропорционалната тежест върху жените. Акцентът трябва да се постави и върху предотвратяването на някои форми на отмъщението, като сексуален тормоз или сексуално изнудване, и повишаването на осведомеността относно половите

Гл. 1 ➤

⁸⁴ 2021 Global Corruption Barometer by Transparency International

⁸⁵ 2021 Global Corruption Barometer by Transparency International

⁸⁶ Виж също: https://knowledgehub.transparency.org/assets/uploads/helpdesk/Gender-sensitivity-in-corruption-reporting-and-whistleblowing_2020_PR.pdf

⁸⁷ Donini, V. M., Lostorto, V., & Zamaro, N. (2022). *Formare per trasformare: l'impatto trasformativo della formazione sulla prevenzione della corruzione. Prime riflessioni. Rivista di diritto amministrativo – Amministrativamente*, 4(2022). <https://www.amministrativamente.com/index.php/formez/article/view/13339>

стереотипи, предразсъдъците и специфичните уязвимости, които засягат лицата, подаващи сигнали за нередности в маргинализирани ситуации.

■ **създаване на рамка за мониторинг, оценка и обучение (MEL – Monitoring, Evaluation and Learning) относно практики за подаване на сигнали, чувствителни към особеностите на пола:**

- редовно извършване на одити, за да се гарантира, че системите за сигнализиране наистина поддържат поверителността, анонимността и защитата от ответни действия с цел отмъщение, особено в случаи, основани на пола;
- провеждане на чувствителни към особеностите на пола оценки на въздействието, за да се оцени дали защитата на лицата, сигнализиращи за нередности, ефективно подкрепя жените, ЛГБТК+ лицата и други уязвими групи;
- създаване на механизъм за обратна връзка, при който лицата, подаващи сигнали за нередности, могат анонимно да съобщават за проблеми със системата, осигурявайки непрекъснато подобрене.

Тези мерки ще помогнат за оценка на ефективността на чувствителните към особеностите на пола защити в рамките на системата за подаване на сигнали за нередности, като се гарантира, че системата непрекъснато се развива за по-добра защита на всички лица, сигнализиращи за нередности, особено тези, които съобщават за неправомерно поведение, основано на пола.

6 ПРЕПОРЪКИ ОТНОСНО РАВЕНСТВОТО МЕЖДУ ПОЛОВЕТЕ И ОТКРИТОТО УПРАВЛЕНИЕ

Глава 6

6.1 ФОКУС ВЪРХУ ОСОБЕНОСТИТЕ НА ПОЛА

Необходимо е ефективно прилагане на политики за защита на лицата, сигнализиращи за нередности, които интегрират **чувствителни към особеностите на пола канали** както на организационно, така и на външно ниво. От съществено значение е да се преодолеят пропуските в съществуващите разпоредби, като например Директивата на ЕС за защита на лицата, сигнализиращи за нередности, и съществуващата национална правна рамка, в които изрично не се **разглеждат аспектите, свързани с пола**.

В този смисъл:

- Международните, националните и местните регулаторни рамки следва да засилят мерките за **създаване на подходящи механизми за защита на жените**, подаващи сигнали за нередности, както и на други уязвими групи.
- Необходимо е да се гарантира, че **каналите за сигнализиране са достъпни**, приобщаващи и отговарят на техните специфични нужди и рискове.
- Следва да се укрепят механизмите за събиране и анализ на данни, за да се осигури по-добро разбиране на поведението, нуждите и приоритетите на лицата, подаващи сигнали за нередности.
- Използването на **чувствителни към особеностите на пола канали и прилагането на целенасочени политики** би повишило ефективността на процесите на подкрепа, особено за жените и други уязвими групи. Нужно е също да се гарантира, че процедурите за сигнализиране, разследване и решаване на случаите дават възможност за справяне с междусекторните неравенства.
- **Трябва да се засилят чувствителните към особеностите на пола мерки за сигурност и поверителност в системите за подаване на сигнали**, както и да се гарантира, че те предвиждат персонализирана защита от неправомерно поведение, основано на пола, гаранции за анонимността на сигнализиращите лица и предотвратяване на ответни действия, особено в ситуации на дисбаланс на силите.
- В случаите на сигнали, основани на пола, следва да се прилагат на протоколи за поверителност за защита на самоличността и предотвратяване на непряка идентификация.
- Необходимо е **разработване на обучения и повишаване на информираността относно чувствителното към особеностите на**

пола подаване на сигнали като превантивна мярка, за да се образуват всички участници в процеса по подаване на сигнали относно особеностите на пола и пресечната точка на други фактори на уязвимост.

Програмата следва да:

- разглежда сигналите за **тормоз, сексуално насилие** и неправомерно поведение, свързано с корупция;
- отчита **различното въздействие върху жените и мъжете**, особено непропорционалната тежест върху жените;
- се фокусира върху **предотвратяването на ответни действия с цел отмъщение**, като сексуален тормоз или сексуално изнудване, и повишаването на информираността относно половите стереотипи, предразсъдъците и специфичните уязвимости, които засягат лицата, сигнализиращи за нередности от маргинализирани групи.

6.2 ФОКУС ВЪРХУ ОТВОРЕНОТО УПРАВЛЕНИЕ

Необходимо е ефективно прилагане на политики за защита на лицата, сигнализиращи за нередности, които интегрират принципите на отвореното управление като прозрачност, участие, отчетност и приобщаване. От съществено значение е да се преодолеят пропуските в съществуващите разпоредби и практики, особено когато системите за подаване на сигнали са неясни, недостъпни или недобре поддържани както от институциите, така и от гражданското общество.

В този смисъл:

- Международните, националните и местните регулаторни рамки следва да засилят **многостранното сътрудничество за съвместно проектиране и наблюдение на системи за подаване на сигнали за нередности**, които съчетават институционалните перспективи с опита и експертния капацитет на организациите на гражданското общество, за да се гарантира яснота, достъпност и доверие в процеса на подаване на сигнали.
- Заинтересованите страни – институции и структури на гражданското общество, следва да работят заедно, за да гарантират, че **каналите за сигнализиране са разбираеми, приобщаващи и проектирани с мисъл за потребителя**, като използват опростен език, практически примери и ясни инструкции по време на целия процес на подаване на сигнали, включително повтарящи се насоки и лесни за ползване формуляри.
- Механизмите за събиране и анализ на данни относно практиките за подаване на сигнали следва да се укрепят, като се гарантира, че **данните се публикуват в отворен формат и се използват за информиране на политиките** чрез прозрачни диалози със заинтересованите страни и повтарящи се цикли на подобрене.
- Трябва да се **прилагат системи за обучение и подкрепа за държавните служители и служителите, разглеждащи вътрешни сигнали**, разработени в сътрудничество между публичните органи и организациите на гражданското общество, които преминават отвъд чисто правния подход и включват експериментално

обучение, основано на етични дилеми и симулации на случаи от реалния живот.

- Необходимо е да се **разработят съвместни комуникационни кампании за повишаване на обществената информираност** относно правата на лицата, сигнализиращи за нередности, и наличните услуги за подкрепа, като се използват националните медии, културни платформи и спортни събития, за да се достигне до разнообразна аудитория.
- Следва да се **насърчават основаните на участие оценки на риска, за да се идентифицират областите на неправомерно поведение**, които са свързани с подаването на сигнали в рамките на институциите, като в процеса се включат както вътрешни участници, така и гражданското общество, за да се гарантира, че системите са максимално съобразени с конкретния контекст.
- Трябва да се **създадат надеждни насоки за защита на данните, разработени съвместно от органите за защита на данните и организациите за подкрепа**, като се гарантира, че лицата, предоставящи услуги по консултиране, могат да обработват лични данни по смислен, но същевременно сигурен начин, балансирайки между поверителността и ефективната подкрепа.
- Необходимо е със **съвместни усилия да бъдат разработени нови закони или подзаконови актове за разширяване на механизмите за защита**, така че да се включат не само лицата, подаващи сигнали, но и тези, които им помагат, като например организации на гражданското общество, правни съветници и журналисти, като се гарантира, че те са защитени от ответни действия, в съответствие с най-добрите международни практики и инструменти за защита на правата на човека.
- Трябва да бъдат **създадени и поддържани публични регистри на граждански и институционални информационни центрове**, като се определят ясни критерии за включване и се насърчава координацията между вписаните в регистрите организации, за да могат лицата, сигнализиращи за нередности, да бъдат ефективно насочвани, както и за да се наблюдават системните предизвикателства чрез редовен обмен на информация.

ОТВЪД РЪКОВОДСТВОТО

Очертава се ключов аспект: **регулаторната рамка** е подобрена благодарение на Директивата на ЕС и нейното транспониране в националните законодателства, но други реформи – някои от тях включени в препоръките в края на предходните глави – могат допълнително да подобрят очакваното въздействие на регулаторната рамка върху доброто управление.

Такъв **политически ангажимент „отгоре надолу“** обаче се нуждае от здрави основи, за да окаже очакваното въздействие върху сложната социална и институционална среда, в която непрекъснато се появяват нови възможности за корупция и злоупотреби. Тези основи се градят върху ценности, принципи, очаквания и доверие. С други думи, културното измерение е от решаващо значение за „овластяването“ на неформалните норми и споделени преценки, които насърчават и подкрепят подаването на сигнали като нормален и ценен компонент на **културата на открито говорене**. Културните особености, които преобладават в определени организации или общества, оказват решаващо влияние върху ефективността на всеки механизъм за **подаване на сигнали за нередности**. В среда, в която корупцията и злоупотребите са „официализирани“ под формата на неписани правила, социалният натиск върху лицата, подаващи сигнали, може да се окаже доминиращ и определящ фактор. Културата очевидно не може да бъде променена със закон, но реформите в законодателството изпращат сигнали, които засягат и социални промени: те могат да „започнат бавен процес“, който с течение на времето да генерира дълбоки промени в начина, по който хората възприемат и преценяват собственото си поведение и поведението на другите. Парадоксалната дилема на сигнализиращото лице е дали ще бъде представено като **„герой или предател“**. Това е точно отражение на съпротивата срещу **нормализиране на практиката** на подаване на сигнали за нередности, когато това е в обществен интерес. Така се засилва и връзката между подходите, ориентирани към „подаването на сигнали“, и тези, ориентирани към „подаващите сигнали“, т.е. между формално-институционалното измерение и субективната и ценностно-ориентирана перспектива.

За да бъде подаването на сигнали за нередности ефективно, трябва да се намери точния баланс между противостоящите интереси, очаквания и права на различните участници в процеса, като сигнализиращото лице е само един от тези участници. Съществените предизвикателства, свързани с регулаторната рамка за подаване на сигнали, са ясно очертани в предходните глави. Как да се **сведат до минимум рисковете** от ответни действия, как да се гарантира правото на неприкосновеност на личния живот и да се **защитят чувствителните данни**, и как да се **проверява съдържанието** на сигналите, например, са сложни въпроси. Цифровите иновации представляват както възможности, така и предизвикателства: онлайн платформите и сигурните канали за комуникация могат да улеснят **анонимното сигнализиране** и да подобрят защитата, но също така **пораждат опасения относно сигурността на данните** и възможността за

злоупотреба. Намирането на баланс между предимствата на цифровите технологии и необходимостта от защита на чувствителната информация е **критичен въпрос**. С други думи, тук не може да се приложи универсална формула: регулирането на подаването на сигнали трябва да даде възможност на всяка публична или частна организация – с присъщите си характеристики и среда – да приспособи своя конкретна и специфична за контекста комбинация от насърчителни мерки, ограничения, обучения, правоприлагане.

Подаването на сигнали има огромен потенциал като инструмент за борба с корупцията. Неговата ефективност обаче зависи от справянето с тези предизвикателства. Задълбоченият емпиричен анализ на моралните и мотивационни основи подаването на сигнали за нередности изглежда необходим източник на знания за подобряване на начина, по който се **възприема ефективността** на съответните политики. Освен това е необходимо да се проучи ролята на етичното обучение и образователните инструменти. Последните всъщност трябва да бъдат ефективен инструмент за сближаване на ценностите на хората, чрез които те се социализират в кръговете на социално признание в публичните и частните организации, с правилата и процедурите, ориентирани към обществения интерес. Когато преобладава определена **обществена стигма** към ролята на сигнализиращото лице, дори и най-сложните платформи за поверително или анонимно сигнализиране ще бъдат безполезни. Постоянната дейност по „**етично обучение**“ в рамките на публичните институции, както и в частните организации, може да изиграе **решаваща роля** в това отношение. Този ангажимент следва да бъде насочен към укрепване на социалните вериги на взаимно признаване и **положително „засилване“** на лоялността спрямо целите на публичните и частните организации, консолидиране на моралните бариери срещу корупцията и етичните мотиви за сигнализиране за нарушения.

В заключение, изглежда необходимо да се **преразгледа социалното измерение**, в рамките на което с течение на времето се оформят източниците на морално признание, които са основната движеща сила зад решението за подаване на сигнал. В крайна сметка успехът на регулирането и законодателството за подаване на сигнали зависи преди всичко от координацията в рамките на една по-широка колективна антикорупционна дейност „**отдолу**“, включваща всички най-важни социални кръгове – както в работната среда, така и в професионалната, организационната, политическата, синдикалната, религиозната и други сфери. Само последното всъщност може да бъде катализатор за **културна промяна**, т.е. обвързваща рамка от убеждения и неформални норми, в която подаването на сигнали за нередности се насърчава и подкрепя чрез публично изразяване на положителни етични оценки за неговите социално полезни ефекти.

ПРИЛОЖЕНИЕ I: МЕТОДОЛОГИЯ НА ИЗСЛЕДВАНЕТО И СЪБИРАНЕ НА ДАННИ

Това ръководство е резултат от експертния опит на всеки партньор в областта на подаването на сигнали за нередности, както и на изследване, проведено с комбинация от методи в периода от юни 2024 г. до ноември 2024 г., включващо четири ключови фази:

1. Кабинетно проучване и изследване на литературата

На този етап е проучена концептуалната и регулаторна рамка за защита на лицата, сигнализиращи за нередности, с акцент върху преглед на задълженията, нивото на прилагане и съществуващите пропуски.

2. Анализ и картографиране на заинтересованите страни

На този стадий са идентифицирани и картографирани над петдесет основни заинтересовани страни, сред които организации на гражданското общество, институции, компании от частния сектор, медии, представители на академичните среди и синдикати. Това са субектите, които биха могли да повлияят или имат отношение към популяризиране на законодателството и повишаване на осведомеността относно подаването на сигнали за нередности. Базата данни със заинтересованите страни е и основата за изготвяне на списък с организациите, които да бъдат включени в качественото изследване и интервютата.

3. Интервюта с ключови експерти

В тази фаза бяха интервюирани представители на най-малко пет организации и институции от всяка страна, за да се събере информация за основните предизвикателства, възможности, препоръки и насоки. Сценарият за провеждане на интервютата се основава на темите, включени в настоящото ръководство, но е използван методът на полуструктурираното интервю, за да се адаптират интервютата към профила на интервюираните. Това е особено полезно за проучване на иновативни и изчерпателни практики, които може да не са били взети предвид при съставянето на въпросниците. Всяко интервю е проведено след получаване на официално съгласие от интервюираното лице в съответствие с изискванията за защита на данните. По време на интервютата се извършва и аудиозапис.

4. Анализ

Интервютата са анализирани в обобщен формат, който позволява да се свърже съдържанието на интервюто с всяка от главите на ръководството, като се набляга на следните ключови теми:

- съществуващи добри практики, прилагани или цитирани от интервюираната организация;
- нужди и предизвикателства, идентифицирани от интервюираното лице във връзка с темите на отделните глави;
- предложения или ключови насоки за действие за подобряване на съществуващото положение.

Освен това основните теми, идентифицирани по време на интервютата, са събрани и обобщени в отделен файл в Excel формат.

ПРИЛОЖЕНИЕ II: СЪКРАЩЕНИЯ

ДФЕС: Договор за функционирането на Европейския съюз

ЕКПЧ: Европейска конвенция за правата на човека

ЕС: Европейски съюз

ИТ: Информационни технологии

ООН: Организация на обединените нации

СЗО: Световна здравна организация

ANAC: Autorità nazionale anticorruzione / Национален орган за борба с корупцията

CAWI: Computer-Assisted Web Interviewing

CATI: Computer-Assisted Telephone Interviewing

CPDP: Commission for Personal Data Protection / Комисия за защита на личните данни

DPO: Data protection officer / Длъжностно лице по защита на данните

GDPR: General Data Protection Regulation / Общ регламент за защита на данните

SLAPP: Strategic Lawsuits Against Public Participation / Стратегически съдебни дела срещу публично участие

SNA: National School of Administration

UNCAC: United Nations Convention against Corruption / Конвенция на ООН срещу корупцията

UNODC: United Nations Office on Drugs and Crime / Служба за борба срещу наркотиците и престъпността на ООН

VLDP: Very Large Online Platform / Много голяма онлайн платформа

VLOSE: Very Large Online Search Engine / Много голяма онлайн търсачка

WCAG: Web Content Accessibility Guidelines / Насоки за достъпност на уеб съдържанието

W3C: World Wide Web Consortium

WMS: Whistleblowing Management Systems / Система за управление на сигнали за нередности



ПРАКТИЧЕСКО РЪКОВОДСТВО ЗА ПОДАВАНЕ НА СИГНАЛИ



Съфинансирано от
Европейския съюз