

Име на процеса/ Name of process	ПРАВИЛА НА „ИНТЕРМЕДИКА ГРУП“ ЕООД ЗА ВЪТРЕШНО ПОДАВАНЕ НА СИГНАЛИ И ЗА ПОСЛЕДВАЩИ ДЕЙСТВИЯ ПО ТЯХ / INTERMEDICA POLICY ON INTERNAL WHISTLEBLOWING AND FOLLOW-UP ACTIONS
Версия/дата / Version/date	03/03.2026
Утвърдил / Approved by	Димитър Иванов, Управител / Dimitar Ivanov, General Manager

I. ПРЕДМЕТ И ЦЕЛ	I. SCOPE AND PURPOSE
Чл. 1. (1) „ИНТЕРМЕДИКА ГРУП“ ЕООД („Дружеството“) осъществява своята дейност честно, почтено и законосъобразно. Като част от мерките да гарантира това и в изпълнение на изискванията на Закона за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения и Директива (ЕС) 2019/1937 на Европейския парламент и на Съвета от 23 октомври 2019 година относно защитата на лицата, които подават сигнали за нарушения на правото на съюза (т.нар. Whistleblower Directive), прие настоящите Правила на „ИНТЕРМЕДИКА ГРУП“ ЕООД за вътрешно подаване на сигнали и за последващи действия по тях („Правилата“). (2) Целта на настоящите Правила е да се създаде рамка за насърчаване на отговорно споделяне на информация за неправомерни или неетични действия, като: ✓ насърчава споделянето, при наличие на знание, за неправомерни или неетични действия, както са описани в Правилата; ✓ урежда реда и условията за организиране на вътрешен канал за подаване на сигнали за Нарушения; ✓ указва как да се подават сигнали за Нарушения и реда за последващи действия по тях; ✓ дефинира мерките насочени към запазване на поверителността и гаранциите, че Нарушения могат да се	Art. 1. (1) INTERMEDICA GROUP EOOD („the Company“) exercises its business with honesty, integrity and in a lawful manner. As part of the measures to ensure this and in fulfillment of the requirements of the Law for protection of persons who report or publicly disclose information about breaches and Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (the so-called Whistleblowing Directive), the company adopted these INTERMEDICA GROUP EOOD Policy on internal whistleblowing and follow-up actions („the Policy“). (2) The purpose of this Policy is to create a framework for promoting responsible sharing of information about misconduct or unethical actions by: ✓ promoting the sharing, in the case of such knowledge, of misconduct or unethical actions as described in the Policy; ✓ setting out the terms and conditions for organizing an internal channel for reporting of Breaches; ✓ providing guidelines on how to report Breaches and the procedure for follow-up actions; ✓ defining the measures for protecting confidentiality and guarantees that Breaches can be reported without fear of retaliation if the report is submitted in good faith.



докладват без страх от ответни мерки, ако се докладва добросъвестно.	
II. ОПРЕДЕЛЕНИЯ И АБРЕВИАТУРИ	II. DEFINITIONS AND ABBREVIATIONS
Чл. 2. За целите на настоящите Правила се прилагат следните определения и аббревиатури: "Нарушения" са действия или бездействия, в Работен контекст, които: са незаконосъобразни и са свързани с българското законодателство или актовете на Европейския съюз в областите, посочени в чл. 5 от Правилата или противоречат на предмета или целта на правилата в актовете на Европейския съюз и областите както е посочено в чл.5 от Правилата; "Нередности" са действия или бездействия, в Работен контекст, които не са Нарушения по смисъла на предходния параграф, но нарушават или заобикалят професионални стандарти и/или етични норми; включително чрез нарушение на вътрешни политики, правила и процедури на Дружеството; "Сигнализиращо лице" означава физическо лице, което подава сигнал или публично оповестява информация за Нарушение, което е узнало в Работен контекст в едно от качествата посочени в чл. 3, ал.1 от настоящите Правила – т.нар. „whistleblower”. "Засегнато лице" означава физическо или юридическо лице, което се посочва при подаването на сигнала или при публичното оповестяване на информация като лице, на което се приписва Нарушението или с което това лице е свързано. "Отговорно лице" означава лице, определено по реда на чл. 12. "Комисия" означава колективния орган, определен по реда на чл. 18. "Работен контекст" означава текущи или минали работни или договорни дейности в/с Дружеството, чрез които, независимо от естеството на тези дейности, лицата придобиват информация за Нарушения и в рамките на които тези лица могат да бъдат подложени на ответни действия с цел отмъщение, ако подадат сигнал с такава информация.	Art. 2. The following definitions and abbreviations shall apply to this Policy: "Breaches" are actions or omissions in Work-related Context, which: are unlawful and related to the Bulgarian legislation or the legislation of the European Union in the fields indicated in Art. 5 of the Policy or which are contrary to the scope and purpose of the provisions of European Union legislation in the areas indicated in Art. 5 of the Policy; "Irregularities" are actions or omissions in Work-related Context, which are not Breaches within the meaning of the previous paragraph, which, however, violate or circumvent any professional standards or codes of conduct, including by violating internal policies, regulations and procedures of the Company; "Whistleblower" means a natural person who submits a report or publicly discloses information about a Breach the person has become aware of in Work-related Context in one of the capacities as defined in Art. 3, para. 1 of this Policy – the so-called "whistleblower". "Concerned Person" means a natural or legal person indicated in the report or public disclosure of information as a person whom the Breach is attributed to or a person whom the Breach is related to. "Responsible Person" means a person defined in the provisions of Art. 12. "Commission" means the collective body defined in the provisions of Art. 18. "Work-related Context" means current or past work-related or contractual activities in/with the Company by means of which, regardless of the nature of these activities, the persons acquire information about Breaches and where these persons could be subject to retaliation for the purpose of revenge if they submit a report with such information. "Personal Data" means any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, by



„Лични данни“ означава всяка информация, която може да бъде свързана с физическо лице, което е идентифицирано или физическо лице, което би могло да бъде идентифицирано, пряко или непряко, чрез използването на един или повече специфични признаци или идентификатори, свързани с това физическо лице, като например име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това лице. От гледна точка на естеството на информацията понятието „лични данни“ включва всеки вид твърдение за едно лице. То включва „обективна“ информация и „субективна“ информация, мнения или оценки. По отношение на формата или носителя, на който се съдържа тази информация, понятието „лични данни“ включва информация под каквато и да е форма, било то азбучна, цифрова, графична, фотографска или акустична. Например то, включва информация, съхранявана на хартия, както и информация, съхранявана в компютърна памет. „ЗЗЛПСПОИН“ означава Закон за защита на лицата подаващи сигнали или публично оповестяващи информация за нарушения. „КЗЛД“ означава Комисията за защита на лични данни.	reference to one or more specific characteristics or identifiers, such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, psychic, mental, economic, cultural or social identity of that person. Regarding the nature of the information, the term “personal data” shall include any type of statement about a person. The concept covers both “objective” and “subjective” information, as well as opinions or evaluations. Regarding the form or the media where this information is contained, the concept of “personal data” shall include information in any form, whether alphabetical, digital, graphic, photographic or acoustic. E.g., this concept includes both information stored on paper and information stored in a computer memory. “LPPWRPDIB“ means Law for protection of persons who report or publicly disclose information about breaches. “CPDP” means the Commission for Personal Data Protection.
III. ПРИЛОЖНО ПОЛЕ Чл. 3 (1) Правилата се прилага за Сигнализиращи лица, подали сигнали за Нарушения, които са придобили информацията в Работен контекст, включително: а) служители по трудов или граждански договор към Дружеството или друго лице, което полага наемен труд, независимо от характера на работата, от начина на заплащането и от източника на финансирането, вкл. стажанти, доброволци; б) лица със статут на самостоятелно заето лице, които са ангажирани с дейността на Дружеството;	III. SCOPE OF APPLICATION Art. 3 (1) This Policy shall apply to Whistleblowers who have reported Breaches and have received the information about them in Work-related Context, including: a) employees hired under employment or civil contract with the Company or other person under paid employment, irrespective of the nature of the work, the method of payment and the source of funding, including interns and volunteers; b) persons with the status of a self-employed person engaged with the Company business; b) partners, shareholders, the sole proprietor of the capital or member of the Company management body;



б) съдружници, акционери, едноличен собственик на капитала, член на управителен орган на Дружеството;

в) изпълнители, подизпълнители, доставчици, други контрагенти, консултанти, одитори, клиенти на Дружеството или лица, които работят при или с тях;

г) Сигнализиращи лица, при които информацията за Нарушения е придобита при работни взаимоотношения, които са приключили, или лица, чиито работни взаимоотношения тепърва предстоят в случаите, когато информацията е получена по време на процеса на набиране на персонал или при други преддоговорни отношения;

д) защита се предоставя и на всяко друго Сигнализиращо лице, което подава сигнал за Нарушение, станало му известно в Работен контекст, съгласно предвиденото в законодателството.

(2) Защита съгласно настоящите Правила се предоставя и на:

а) лица, които помагат на Сигнализиращото лице в процеса на подаване на сигнал;

б) лица, които са свързани със Сигнализиращото лице и които могат да бъдат подложени на репресивни ответни действия поради сигнализирането, като например колеги или роднини;

в) юридически лица, за които сигнализиращото лице работи, на които е собственик или с които е свързано по друг начин в Работен контекст;

Чл. 4. Сигнализиращите лица имат право на защита, съгласно настоящите Правила, при условие, че едновременно:

а) са имали основателна причина да смятат, че подадената информация за Нарушения е била вярна към момента на подаването ѝ и тази информация попада в материалния обхват, съгласно чл. 5 на Правилата и

б) са подали сигнал в съответствие с Правилата по указания ред.

Чл. 5. (1) Настоящите Правила се прилагат по отношение на сигнали за Нарушения на

c) contractors, subcontractors, suppliers, other counterparties, consultants, auditors, customers of the Company or persons working for or with them;

d) Whistleblowers who have acquired the information about Breaches in the context of employment relationships that have ended or persons whose employment relationships are forthcoming, in the cases where the information has been obtained during the process of staff recruitment or other pre-contractual relationships;

e) protection shall also be provided to any other Whistleblower reporting a Breach they have become aware of in Work-related Context as provided for in legislation.

(2) Protection under this Policy shall be also provided to:

a) persons who help the Whistleblower in the process of reporting;

b) persons who have contacted the Whistleblower and who can face retaliation as a result of the report, such as colleagues and relatives;

c) legal entities the Whistleblower works for, owns or is otherwise connected with in a Work-related Context;

Art. 4. Whistleblowers have the right to protection under this Policy, provided that all of the following conditions have been met:

a) they have reasonable grounds to believe that the reported information about Breaches is true at the time of its submission and that this information falls within the material scope of Art. 5 of this Policy; and

b) they have submitted a report in accordance with this Policy according to the specified procedure.

Art. 5. (1) This Policy shall apply to reports about Breaches of the Bulgarian legislation or European Union legislation mentioned in the annex to LPPWRPDIB in the field of:



българското законодателство или на посочените в приложението към ЗЗЛПСПОИН актове на Европейския съюз в областта на: а) обществените поръчки, свързани с дейността на Дружеството; б) финансовите услуги, продукти и пазари и предотвратяването на изпирането на пари и финансирането на тероризма; в) безопасността и съответствието на продуктите; г) безопасността на транспорта; д) опазването на околната среда; е) радиационната защита и ядрената безопасност; ж) безопасността на храните и фуражите, здравето на животните и хуманното отношение към тях; з) общественото здраве; и) защитата на потребителите; к) защитата на неприкосновеността на личния живот и личните данни; л) сигурността на мрежите и информационните системи; (2) Настоящите Правила се прилагат и по отношение на сигнали за: а) нарушения, които засягат финансовите интереси на Европейския съюз по смисъла на чл. 325 от Договора за функционирането на Европейския съюз и допълнително уточнени в съответните мерки на Съюза; б) нарушения на правилата на вътрешния пазар по смисъла на чл. 26, параграф 2 от Договора за функционирането на Европейския съюз, включително правилата на Европейския съюз и българското законодателство относно конкуренцията и държавните помощи; в) нарушения, свързани с трансгранични данъчни схеми, чиято цел е да се получи данъчно предимство, което противоречи на предмета или на целта на приложимото право в областта на корпоративното данъчно облагане; г) извършено престъпление от общ характер, за което Сигнализиращото лице е узнало във връзка с извършване на своята работа или при изпълнение на служебните си задължения.	а) public procurement related to the Company's activity; б) financial services, products and markets and prevention of money laundering and terrorist financing; с) product safety and compliance; д) safety of transport; е) protection of the environment; ф) radiation protection and nuclear safety; г) food and feed safety, animal health and welfare; х) public health; и) consumer protection; к) protection of privacy and personal data; л) security of network and information systems. (2) This Policy shall also apply to reports about: а) breaches affecting the financial interests of the European Union within the meaning of Art. 325 of the Treaty on the Functioning of the European Union and further specified in the relevant Union measures; б) breaches of the internal market rules within the meaning of Art. 26(2) of the Treaty on the Functioning of the European Union, including the regulations of the European Union and Bulgarian legislation with respect to competition and state aid; с) breaches related to cross-border tax schemes aimed at obtaining a tax advantage that defeats the object or purpose of the applicable corporate tax law; д) general criminal offense committed which the Whistleblower has become aware of in relation to the performance of their work or during the fulfillment of their job duties.
--	---



(3) Настоящите правила се прилагат и по отношение на сигнали за Нарушения на българското законодателство в областта на: а) правилата за заплащане на дължими публични държавни и общински вземания; б) българското трудово законодателство; в) изпълнението на държавна служба. Чл. 6. Не се образува производство по анонимни сигнали. Чл. 7. (1) Всеки служител или лице, посочено в чл.3. от тези Правила може да сигнализира също и за нередности или неетични действия, извън обхвата на ЗЗЛПСПОИН, т.е. такива които не представляват Нарушения, не водят пряко или косвено до Нарушение, вкл. не застрашават или увреждат обществен интерес, като използва вътрешните канали описани в чл.11, без да е необходимо да се спазва изискването за ползване на формуляра представляващ Приложение № 1 или цялата информация посочена в него. (2) Такива действия могат да бъдат например: ✓ несъобразяване с принципите и разпоредбите на Етичния кодекс на Дружеството или на други разпоредби на вътрешни правила на Дружеството; ✓ използване/разпространение на вътрешна или друг вид конфиденциална информация; ✓ злоупотреба със служебно положение или авторитет; ✓ вербална агресия; ✓ неморално или неетично поведение или злонамерени практики. (3) Дружеството се ангажира да разгледа такъв сигнал справедливо и да предприеме съответни мерки и действия. (4) Разпоредбите на тези Правила и на ЗЗЛПСПОИН не се прилагат, вкл. относно регистриране и разглеждане на сигнала и защитата на лицата подаващи сигнали за Нарушения.	(3) This Policy shall also apply to reports about Breaches of the Bulgarian legislation in the field of: a) the regulation on payment of public state or municipal receivables due; b) the Bulgarian labor legislation; c) performance of public service. Art. 6. No proceedings shall be initiated based on anonymous reports. Art. 7. (1) Each employee or person under Art. 3 of this Policy may also report irregularities or misconduct outside the scope of LPPWRPDIB, i.e. actions that do not constitute Breaches, do not cause, directly or indirectly, a Breach, including actions that do not threaten or harm the public interest, by using the internal channels described in Art. 11, without the need to comply with the requirement to use the form in Annex No. 1 or provide the entire information specified therein. (2) Such actions, by way of example, may include: ✓ non-compliance with the principles and provisions of the Company Code of Conduct or other provisions or internal regulations of the Company; ✓ use/dissemination of internal or other type of confidential information; ✓ abuse of office or authority; ✓ verbal aggression; ✓ immoral or unethical conduct or malpractices. (3) The Company commits to investigating any such report in a fair manner and to undertake the relevant measures and actions. (4) The provisions of this Policy and of LPPWRPDIB shall not apply, including in respect of recording and review of the report and protection of the Whistleblowers reporting Breaches.
IV. ПОДАВАНЕ НА СИГНАЛИ. КАНАЛИ.	IV. REPORTING. CHANNELS.



Чл. 8. Дружеството насърчава подаване на сигнали до Отговорното лице с цел бързо предотвратяване на Нарушение или отстраняване на последиците от такова (т.нар. „вътрешен канал“ за подаване на сигнали).

Чл. 9. Сигнал, обаче, може да бъде подаден и до КЗЛД, в случай че Сигнализиращото лице има основателно предположение, че за него съществува риск от ответни, дискриминиращи го действия, както и че няма да бъдат предприети ефективни мерки за проверка на сигнала (т. нар. „външен канал“ за подаване на сигнали). Повече информация за подаване на сигнал до КЗЛД може да бъде открита на следния адрес: <https://www.cdpd.bg/>

Чл. 10. Сигнализиращото лице може да оповести публично информацията и да има право на защита по ЗЗЛПСПОИН, когато е имало основателна причина да счита, че информацията за Нарушението е била вярна към момента на оповестяването и че тази информация попада в обхвата на чл. 5 от тези Правила, и е изпълнено някое от следните условия:

а) ако е подало сигнал до Отговорното лице в Дружеството или/и до Комисията за защита на лични данни, но по него не са предприети действия в предвидените срокове;

а) лицето има основание да счита, че:

- Нарушението може да представлява непосредствена или явна опасност за обществен интерес или съществува риск от щети, които не могат да бъдат отстранени или е налице извънредна ситуация или риск от необратими вреди;

- в случай на външно подаване на сигнал до КЗЛД съществува риск от ответни действия или има вероятност Нарушението да не бъде ефективно разгледано поради опасност от укриване или унищожаване на доказателства, съмнение за наличие на тайно споразумение между КЗЛД и извършителя на Нарушението, или за съучастие на КЗЛД в Нарушението, както и поради други специфични конкретни обстоятелства по случая.

Art. 8. The Company encourages reporting to the Responsible Person for the purpose of rapid prevention of a Breach or elimination of the consequences thereof (the so-called “internal channel” for reporting).

Art. 9. A report, however, may also be submitted to CPDP, if the Whistleblower has the ground to assume they would face a risk of retaliation or discriminatory actions and that no effective measures for inspection of the report will be undertaken (the so-called “external channel” for reporting). More information about submitting a report to CPDP can be found on the following address: <https://www.cdpd.bg/>

Art. 10. The Whistleblower may disclose the information publicly and may be entitled to protection under LPPWRPDIB where there is a reasonable ground to believe that the information about the Breach was true at the time of disclosure and that this information fell within the scope of Art. 5 of this Policy and any of the following conditions was met:

a) if the report was submitted to the Responsible Person in the Company and/or the Commission of Personal Data Protection, but no actions were undertaken in respect thereof within the envisaged periods;

a) the person has the ground to believe that:

- the Breach may constitute an imminent or manifest danger to the public interest or there is a risk of damages that cannot be removed or there is an extraordinary situation or risk of irreversible damage;

- in the case of external submission of a report to CPDP, there is a risk of retaliation or it is likely that the Breach will not be effectively reviewed due to a risk of concealing or destroying evidence, suspicion for the presence of a collusion between CPDP and the perpetrator or for complicity of CPDP in committing the Breach or any other specific circumstances related to the case.



Чл. 11. (1) Сигнали за Нарушения могат да се подават на следните специални канали за подаване на сигнал, осигурени от Дружеството:

1. чрез електронна поща на адрес - whistleblower@intermedica.eu необходимо е сигналът (формулярът) да бъде подписан с квалифициран електронен подпис (КЕП) на Сигнализиращото лице;

2. писмено, чрез лично предаване на Отговорното лице или по куриер или чрез пощенска пратка на адрес: гр. София, бул. „Цариградско шосе“ № 361 и под адресата „Интермедика Груп“ ЕООД е изписан текст „сигнал по ЗЗЛПСПОИН“ - необходимо е сигналът (формулярът) да бъде саморъчно подписан от подаващото го лице;

3. устно на Отговорното лице като се свържете на телефона посочен в чл. 32 по-долу от 9:00 до 12:00 часа в работни дни включително чрез система за гласови съобщения, или чрез лична среща с Отговорното лице, уговорена предварително на посочения телефон;

Устният сигнал се документира чрез попълване на формуляра по образец от Отговорното лице. На Сигнализиращото лице се предлага да го провери, коригира и одобри, като го подпише. Ако лицето, подаващо сигнала, не подпише формуляра, сигналът се приравнява на анонимен.

В случай на лична среща със Сигнализиращото лице, срещите се провеждат само в присъствието на Сигнализиращото лице и Отговорното лице, а по изключение ако се налага и на един член на Комисията или външно лице, ако е определено такова да подпомага процеса.

При изрично съгласие на лицето, подаващо сигнала, устният сигнал, подаден чрез телефонна линия или друга система за гласови съобщения, или лична среща, може да бъде документиран и посредством запис на траен носител, позволяващ неговото извличане.

(2) Каналите са създадени и управляват по начин, който възпрепятства достъпа до неупълномощени лица до подадени сигнали и гарантира пълнотата, целостта и

Art. 11. (1) Reports about Breaches can be submitted to the following special reporting channels provided by the Company:

1. via electronic mail to the following address: whistleblower@intermedica.eu – the report (form) needs to be signed with qualified electronic signature (QES) of the Whistleblower;

2. in writing, by serving the report to the Responsible Person or sending it via courier or post to the following address: city of Sofia, 361 Tsarigradsko Shose Blvd., 3rd floor, to the attention of INTERMEDICA GROUP EOOD, with the text “report under LPPWRPDIB” - the report (form) needs to be signed by hand by the reporter;

3. verbally to the Responsible Person by contacting them at the telephone number indicated in Art. 32 below between 9:00 a.m. and 12:00 p.m. during business days, including through the voicemail system, or by arranging a meeting in person with the Responsible Person scheduled in advance via the indicated telephone number; The verbal report shall be documented by filling out the sample form by the Responsible Person. The Whistleblower will be offered to review, correct and approve it by signing it. If the person submitting the report does not sign the form, the report shall be treated as anonymous.

In the case of a meeting in person with the Whistleblower, the meetings may only be held in the presence of the Whistleblower and the Responsible Person or, in exceptional circumstances, if necessary, in the presence of a member of the Commission or an external party, if such has been determined for the purpose of supporting the process.

With the explicit consent of the person submitting the report, an oral report made via telephone line, other voice messaging system, or in a personal meeting may be documented by means of a durable medium that allows its retrieval.

(2) The channels have been created and are administered in a way that prevents access by unauthorized persons to the reports submitted and guarantee the completeness, integrity and confidentiality of the information and protection of the Personal Data of the Whistleblower, the



поверителността на информацията и защитата на Личните данни на Сигнализиращото лице, Засегнатото лице/а и всяко друго лице засегнато от сигнала. (3) За подаване на сигнали за Нарушения е желателно да се използва формуляр съгласно Приложение № 1 към настоящите Правила, който е по образец на КЗЛД. В случай, че сигналът не е подаден чрез попълване на формуляр, Отговорното лице попълва формуляра като използва информацията от сигнала. При непълноти изисква от Сигнализиращото лице допълнителна информация. (4) Към сигнала могат да се приложат всякакъв вид източници на информация, подкрепящи изложените в него твърдения, и/или позоваване на документи, в т.ч. посочване на данни на лица, които биха могли да потвърдят съобщените данни или да предоставят допълнителна информация.	Concerned Person(s) and/or any other person affected by the report. (3) For submission of reports about Breaches, it is recommended to use the form in Annex No. 1 to this Policy, which was made based on the template of CPDP. If the report has not been submitted by filling out the form, the Responsible Person shall fill out the form based on the information from the report. In the case of incomplete information, they shall request additional information from the Whistleblower. (4) The report can be accompanied by any types of sources of information supporting the statements in it and/or reference to documents, including indication of details about persons who could confirm the reported data or provide additional information.
V. РЕГИСТРИРАНЕ И РАЗГЛЕЖДАНЕ НА СИГНАЛИ	V. RECORDING AND REVIEWING THE REPORTS
Чл. 12. (1) Приемането, регистрирането и потвърждаване на получаването на сигнали за Нарушения се извършва от служител/и в Дружеството или външно лице, ако е допустимо, определено със заповед на представляващия Дружеството, наричано в тези Правила Отговорно лице. (2) В случай на конфликт на интереси на Отговорното лице и подадения към него сигнал, представляващия Дружеството със заповед определя друго лице за обработване и разглеждане на сигнала. (3) Сигнали срещу Отговорното лице се подават до управителя/изпълнителен директор. (4) Сигнали срещу управителя/изпълнителен директор на Дружеството се подават до крайния собственик на компанията/Председателя на Съвета на директорите. (5) Отговорното лице може да бъде подпомогано от външно лице с познания в областта.	Art. 12. (1) The acceptance, recording and acknowledgment of receipt of reports about Breaches shall be performed by Company employee(s) or by a third party, if admissible, appointed by an order of the Company representative, referred to as the Responsible Person in this Policy. (2) In the case of conflict of interests between the Responsible Person and the report submitted to them, the Company representative shall issue an order to appoint another person for processing and reviewing the report. (3) Reports against the Responsible Person shall be submitted to the general manager/chief executive officer. (4) Reports against the general manager/chief executive officer of the Company shall be submitted to the beneficial owner of the Company/Chair of the Board of Directors. (5) The Responsible Person may receive support from an external person with knowledge in the relevant field.



Чл. 13. (1) В 7-дневен срок от получаването на сигнала, Отговорното лице извършва проверка за редовност на сигнала и ако сигналът не отговаря на изискванията на тези Правила и ЗЗЛПСПОИН, на Сигнализиращото лице се изпраща съобщение за отстраняване на допуснатите нередности в 7-дневен срок от получаване на сигнала.

(2) Ако нередностите по сигнала не бъдат отстранени в срок, Отговорното лице връща сигнала на Сигнализиращото лице, заедно с приложенията към него.

Чл. 14. (1) Отговорното лице проверява сигнала и по отношение на неговата достоверност. Не се разглеждат сигнали, които не дават основания да се приемат за правдоподобни.

(2) Сигнали, които съдържат очевидно неверни или заблуждаващи твърдения за факти, се връщат с указание към подателя за поправка на твърденията и за отговорността, която той носи за набездаване.

Чл. 15. (1) Отговорното лице проверява и дали сигналът попада в обхвата на Правилата, съгласно чл.5 по-горе.

(2) В случай, че сигналът не попада в обхвата на чл. 5 по-горе, но попада в обхвата на чл.7 той се разглежда по реда на същия чл.7, съответно и останалите разпоредби на тези Правила и ЗЗЛПСПОИН не се прилагат.

Чл. 16. При постъпване на надлежен сигнал Отговорното лице е длъжно да генерира Уникален идентификационен номер (УИН) в системата на КЗЛД, като компетентен национален орган и в 7-дневен срок да потвърди получаването на сигнала пред Сигнализиращото лице.

Чл. 17. В случай, че сигнал за Нарушения попадне при служител, различен от Отговорното лице, на получилия го служител се забранява да разкрива всякаква информация, чрез която би могла да се установи самоличността на Сигнализиращото или Засегнатото

Art. 13. (1) Within 7 days of receipt of the report, the Responsible Person shall check the regularity of the report and if the report fails to meet the requirements under this Policy and LPPWRPDIB, a message should be sent to the Whistleblower for rectifying the relevant irregularities within 7 days of receipt of the report.

(2) If the irregularities in the report are not rectified within the specified period, the Responsible Person shall return the report, together with the annexes thereto, to the Whistleblower.

Art. 14. (1) The Responsible Person shall also check the credibility of the report. Reports that give no grounds to be considered credible will not be reviewed.

(2) Reports that contain obviously false or misleading statements about any facts will be returned to the sender with an instruction for correction of the statements and a reminder that the sender may be held liable for defamation.

Art. 15. (1) The Responsible Person shall check whether the report falls within the scope of the Policy according to Art. 5 above.

(2) If the report does not fall within the scope of Art. 5 above, but falls within the scope of Art. 7, it shall be reviewed according to the procedure specified in Art. 7 and, respectively, the remaining provisions of this Policy and LPPWRPDIB shall not apply.

Art. 16. Upon receipt of a proper report, the Responsible Person must generate a Unique Identification Number (UIN) in the system of CPDP as the competent national authority and acknowledge the receipt of the report to the Whistleblower within a period of 7 days.

Art. 17. If a report about a Breach is received by an employee other than the Responsible Person, the employee that has received it shall be prohibited from disclosing any information that could identify the Whistleblower or the Concerned



лице, а сигналът се препраща незабавно, без изменения, на Отговорното лице.

Чл. 18. (1) Разглеждането на надлежно постъпилите сигнали се извършва от комисия от служители на Дружеството, определени от представляващия Дружеството.

(2) В случай на конфликт на интереси на член/ове на Комисията и подадения сигнал, или отсъствие на член, което би могло да забави разглеждането, представляващия Дружеството със заповед определя друг/и служител/и в състава на Комисията за разглеждане на сигнала.

(3) Комисията може да бъде подпомагана от външно лице с познания в областта.

Чл. 19. (1) В случай, че сигналът подлежи на разглеждане и Отговорното лице прецени, че е необходимо, Отговорното лице го докладва на Комисията, която Комисия решава какви мерки и действия следва да бъдат предприети.

(2) Комисията може да заседава и непряко чрез средства за отдалечена комуникация.

(3) За взетите от Комисията решения, Отговорното лице съставя протоколи, които се подписват от него в качеството на секретар на Комисията.

Чл. 20. В срок не-по-дълг от 3 (три) месеца след потвърждаване на получаването на сигнала, Отговорното лице изготвя доклад, в който накратко се описва информацията от сигнала, предприетите действия, окончателните резултати от проверката, които Отговорното лице писмено съобщава на Сигнализиращото лице и на Засегнатото лице, при спазване на задължението за тяхната защита.

Чл. 21. В случай, че изложените в сигнала обстоятелства бъдат потвърдени, Отговорното лице:

а) в случай, че предложените мерки и действия са в компетенциите на Комисията или неин член, или е неговите, отбелязва кой/кои

Person and the report shall be forwarded immediately, without any changes, to the Responsible Person.

Art. 18. (1) Properly received reports shall be reviewed by a commission of Company employees determined by the Company representative.

(2) In the case of conflicts of interests between any member(s) of the Commission and the report sent or absence of a member that could delay the review, the Company representative shall issue an order to appoint other employee(s) in the composition of the Commission for reviewing the report.

(3) The Commission may receive support from an external person with knowledge in the relevant field.

Art. 19. (1) If the report is deemed to be subject to review and the Responsible Person deems necessary, they shall report it to the Commission, which shall decide on the measures and actions to be undertaken.

(2) The Commission may also meet in absentia by using remote communication tools.

(3) The Responsible Person shall draft minutes for the decisions taken by the Commission, which shall be signed by the responsible person in their capacity as secretary of the Commission.

Art. 20. Within no more than 3 (three) months after acknowledgment of receipt of the report, the Responsible Person shall draft a report briefly describing the information from the report, the actions undertaken, the final results from the inspection and the Responsible Person shall communicate this report in writing to the Whistleblower and to the Concerned Person, while complying with the obligation to ensure their protection.

Art. 21. If the circumstances detailed in the report are confirmed, the Responsible Person:

a) shall note the responsible person(s) for undertaking the relevant measures and actions and shall order their implementation, if the proposed



лица са отговорни за предприемане на съответните мерки и действия и нарежда предприемането им;

б) изготвя и представя на представляващия Дружеството доклад, в който се съдържа информация за сигнала, предприетите последващи действия и предложение за предприемане на конкретни мерки и действия от компетентността на представляващия Дружеството с цел преустановяване или предотвратяване на Нарушението.

в) насочва Сигнализиращото лице към компетентните органи, когато се засягат неговите права;

в) препраща сигнала към КЗЛД като орган за външно подаване на сигнали при необходимост от предприемане на действия от предприемане на действия от негова страна, като за препращането Сигнализиращото лице се уведомява предварително; в случай че сигналът е подаден срещу работодателя на Сигнализиращото лице, Отговорното лице насочва Сигнализиращото лице за едновременно сигнализиране на органа за външно подаване на сигнали.

Чл. 22. (1) Проверката се прекратява, когато Нарушението е маловажен случай, по отношение на нарушението са изтекли предвидените в съответния закон срокове за образуване на административнонаказателно или наказателно производство, съответно административнонаказателната или наказателната отговорност е погасена поради изтичане на предвидената в съответния закон давност, по повтарящ се сигнал, който не съдържа нова информация от съществено значение за Нарушението, както и когато се установят данни за извършено престъпление.

(2) Отговорното лице изготвя проект на уведомление до Сигнализиращото лице, в което излага основанията и мотивите за прекратяване на проверката по сигнала. Отговорното лице изпраща уведомлението до Сигнализиращото лице.

(3) При прекратяване на проверката по реда на този член, Сигнализиращо лице може да подаде сигнал до КЗЛД.

measures and actions are within the competence of the Commission or a member thereof or within the competence of the Responsible Person;

b) shall draft and present a report to the Company representative containing information about the report, the subsequent actions undertaken and a proposal for undertaking specific measures and actions within the competence of the Company representative for the purpose of discontinuing or preventing the Breach.

c) shall refer the Whistleblower to the competent authorities when their rights are affected;

c) shall forward the report to CPDP as the authority for external reporting if actions need to be undertaken by this authority and shall notify the Whistleblower in advance about such forwarding; if the report has been submitted against the Whistleblower's employer, the Responsible Person shall refer the Whistleblower for simultaneous reporting to the authority for external reporting.

Art. 22. (1) The inspection shall be discontinued if the Breach is a minor case, when the statutory time limits for initiating administrative or criminal proceedings in respect of the violation have expired, or when the administrative or criminal liability has been extinguished due to the expiration of the limitation period provided for by the applicable law, if the case concerns a repeated report that does not contain new information of material importance for the Breach or if information that an offense has been committed is obtained.

(2) The Responsible Person shall draft a notification to the Whistleblower, detailing the ground and justification to discontinue the inspection on the report. The Responsible Person shall send the notification to the Whistleblower.

(3) After discontinuation of the inspection according to the provisions of this article, the Whistleblower may submit a report to CPDP.



Чл. 23. Когато в хода на проверката се установени данни за извършено престъпление, сигналът и материалите към него се изпращат незабавно на прокуратурата.	Art. 23. If, in the course of the inspection, evidence for a committed criminal offense is found, the report and the materials thereto shall be immediately sent to the prosecutor's office.
VI. РЕГИСТЪР НА СИГНАЛИТЕ. СЪХРАНЯВАНЕ НА ДОКУМЕНТИ	VI. RECORD OF REPORTS. STORAGE OF DOCUMENTS
Чл. 24. (1) В Дружеството се създава и поддържа електронен Регистър на сигналите по образец, утвърден от КЗЛД, съгласно Приложение № 2. (2) Регистърът не е публичен. (3) Регистърът се води от Отговорното лице. Чл. 25. (1) Електронните документи, свързани със сигнали, се обработват, съхраняват и организират в специално създадени за целта електронни папки, по начин, който гарантира тяхната поверителност и сигурност. (2) Отговорното лице и членовете на Комисията имат право да обработват документи свързани със сигнали само на служебни устройства, защитени с парола и отговарящи на изискванията за сигурност в Дружеството. Чл. 26. (1) Документите на хартиен носител свързани със сигнали се обработват и съхраняват по начин, който гарантира тяхната поверителност и сигурност. (2) Хартиените носители се съхраняват в отделен архив, с ограничен достъп само за Отговорното лице чрез ключ. (3) Отговорното лице и членовете на Комисията нямат право да оставят на работното си място без надзор документи и носители на информация, свързани със сигнали. Чл. 27. (1) Сигналите и всички съпътстващи ги документи се съхраняват за срок от 5 години след приключване на разглеждането на сигнала, освен при наличието на образувано наказателно, гражданско, трудовоправно и/или административно производство във връзка с подадения сигнал.	Art. 24. (1) The Company shall create and maintain an electronic record of the reports based on a template approved by CPDP and contained in Annex No. 2. (2) This record shall not be public. (3) The record shall be kept by the Responsible Person. Art. 25. (1) Any electronic documents related to reports shall be processed, stored and organized in designated electronic files in a way that guarantees their confidentiality and security. (3) The Responsible Person and the members of the Commission shall have the right to process documents related to reports only on password-protected company devices that meet the security requirements of the Company. Art. 26. (1) Any documents on paper related to reports shall be processed and stored in a way that guarantees their confidentiality and security. (2) Paper documents shall be stored in a separate archive with access thereto limited to only the Responsible Person by means of a key. (3) The Responsible Person and the members of the Commission shall have no right to leave documents and media containing information related to reports unattended at their work place. Art. 27. (1) The reports and all accompanying documents shall be stored for a period of 5 years after finalization of the review of the report, unless proceedings have been initiated under criminal, civil, employment and/or administrative law in relation to the report submitted. (2) After expiration of the storage period, the data shall be destroyed by the retaining person



(2) След изтичане на срока за съхранение, данните се унищожават от държащото ги лице чрез трайно унищожаване с невъзможност да се възстановят.	through permanent destruction without any possibility for recovery.
VII. ЗАЩИТА НА ЛИЦАТА, ПОДАВАЩИ СИГНАЛИ ЗА НАРУШЕНИЯ	VII. PROTECTION OF WHISTLEBLOWERS REPORTING BREACHES
Чл. 28. (1) Дружеството предприема мерки за защита на информацията, свързана с подадените сигнали за Нарушения, и за защита на самоличността на Сигнализиращите лица, Засегнатите лица и всяко друго лице упоменато в сигнал, като осигурява достъп до информацията единствено на служителите, на които тези данни са необходими за изпълняване на служебните им задължения (това са Отговорното лице и членовете на Комисията). (2) Разкриването на самоличността на Сигнализиращото лице се допуска само при изричното му писмено съгласие за това. (3) Независимо от това, съгласно законодателството, самоличността на Сигнализиращото лице и всяка друга информация, от която може пряко или непряко да се узнае неговата самоличност, може да бъде разкрита когато това е необходимо в контекста на разследвания от национални органи или на съдебни производства, включително с оглед на гарантиране правото на защита на Засегнатото лице. В тези случаи, преди разкриването на самоличността или на информацията в сигнала, Дружеството уведомява Сигнализиращото лице за необходимостта от разкриването им. Уведомлението е писмено и се мотивира. Дружеството не уведомява Сигнализиращото лице, когато с това се застрашава разследването или съдебното производство. Чл. 29. (1) Дружеството не толерира по никакъв начин подлагането на Сигнализиращите лица, които действат добросъвестно при подаването на сигнали, на ответни действия от каквото и да било естество, с цел отмъщение. (2) Дружеството предприема всички необходими мерки Сигнализиращите лица, да не	Art. 28. (1) The Company shall undertake measures to protect the information related to the submitted reports about Breaches and to protect the identity of the Whistleblowers, the Concerned Persons and any other person mentioned in a report and shall only provide access to the information to employees who need these data to fulfill their work-related duties (these are the Responsible Person and the members of the Commission). (2) Disclosure of the Whistleblower's identity shall only be allowed after obtaining their written consent about this. (3) Notwithstanding the foregoing, according to the legislation, the identity of the Whistleblower and any other information that could directly or indirectly identify them can be disclosed, where necessary, in the context of investigations performed by national authorities or in relation to judicial proceedings, including with a view to ensuring the right to protection of the Concerned Person. In these cases, the Company shall notify the Whistleblower about the need of such disclosure before disclosing their identity or the information in the report. The notification shall be done in writing and shall be justified. The Company does not need to notify the Whistleblower where this would threaten the investigation or judicial proceedings. Art. 29. (1) The Company does not tolerate any form of retaliation for the purpose of revenge against Whistleblowers who report in good faith. (2) The Company undertakes all the necessary measures so as to ensure that Whistleblowers will not be subject to retaliation having the nature of repression and placing them in an



бъдат обект на ответни действия имащи характера на репресия и поставящи ги в неблагоприятно положение, както и заплахи или опити за такива действия, включително под формата на:

1. временно отстраняване, уволнение или прилагане на друго основание за прекратяване на правоотношението, по което лице полага наемен труд;
2. понижаване в длъжност или забавяне на повишение в длъжност;
3. изменение на мястото или характера на работата, продължителността на работното време или намаляване на възнаграждението;
4. отказ за осигуряване на обучение за поддържане и повишаване на професионалната квалификация на работника или служителя;
5. отрицателна оценка на работата, включително в препоръка за работа;
6. прилагане на имуществена и/или дисциплинарна отговорност, включително налагане на дисциплинарни наказания;
7. принуда, отхвърляне, заплашване за предприемане на ответни действия или действия, изразени физически, словесно или по друг начин, които имат за цел накарване на достойнството на лицето и създаване на враждебна професионална среда;
8. пряка или непряка дискриминация, неравностойно или неблагоприятно третиране;
9. отнемане на възможност за преминаване от срочен трудов договор на трудов договор за неопределено време, когато работникът или служителят е имал законно право да му бъде предложена постоянна работа;
10. предсрочно прекратяване на срочен трудов договор или отказ за повторно сключване, когато такова е допустимо по закон;
11. вреди, включително за репутацията на лицето, по-специално в социалните мрежи, или финансови загуби, включително загуба на бизнес и загуба на доход;
12. включване в списък, изготвен въз основа на официално или неофициално споразумение, в сектор или в отрасъл, което може да доведе до това лицето да не може да постъпи

unfavorable situation or any threats or attempts for such actions, including actions in the form of:

1. Temporary dismissal, termination or application of other ground for ending the paid employment relationship with the person;
2. Demotion or delaying promotion;
3. Change in the place or nature of the work, the duration of the working hours or decrease of remuneration;
4. Refusal to provide training for maintaining or increasing the professional competence of the worker or employee;
5. Negative evaluation of the work, including in a reference letter for work;
6. Imposing financial and/or disciplinary measures, including imposing of disciplinary sanctions;
7. Coercion, rejection, threats to undertake retaliation or actions expressed physically, verbally or otherwise with the purpose of violating the dignity of the person and creating a hostile professional environment;
8. Direct or indirect discrimination, unequal or unfavorable treatment;
9. Depriving the person of the possibility to switch from a fixed-term employment contract to an employment contract for an indefinite period where the worker or employee has had the legal right to be proposed permanent employment;
10. Pre-term termination of a fixed-term employment contract or refusal for renewing the contract, where such is allowed by the law;
11. Damages caused to the person, including to their reputation, especially in social networks, or financial losses, including loss of business and loss of income;
12. Inclusion in a list drafted based on a formal or informal agreement, in a sector or industry, which may prevent the person from starting work or from supplying goods or services in this sector or industry (blacklisting);
13. Pre-term termination or breaking of a contract for provision of goods or services, where the person is a supplier;
14. Termination of a license or authorization;
15. Referring the person for medical examination.



на работа или да не може да достави стока или услуга в този сектор или отрасъл (черен списък); 13. предсрочно прекратяване или разваляне на договор за доставка на стоки или услуги, когато лицето е доставчик; 14. прекратяване на лиценз или разрешение; 15. насочване на лицето към извършване на медицински преглед.	
VIII. ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ	VIII. PERSONAL DATA PROCESSING
Чл. 30. (1) Всяко обработване на Лични данни, включително обмен или предаване на Лични данни от компетентните органи, се извършва в съответствие с Регламент (ЕС) 2016/679 и Директива (ЕС) 2016/680, а когато в предаването участват институции, органи, служби или агенции на Европейския съюз – в съответствие с Регламент (ЕС) 2018/1725, както и със Закона за защита на личните данни. (2) При получаване и разглеждане на сигнали по реда на тези Правила, Дружеството прилага подходящи технически и организационни мерки, съгласно вътрешните си правила и процедури, и приложимото национално и европейско законодателство, които гарантират законосъобразното обработване на Лични данни. (3) Обработването, включително предаването на Лични данни, ще се извършва само до степента, необходима за разследване на сигнала и в съответствие с Регламент (ЕС) 2016/679 и Закона за защита на личните данни. (4) Не се събират Лични данни, които явно не са от значение за разглеждане на конкретния сигнал, а ако бъдат случайно събрани, се заличават. (5) Лични данни, обработени по повод сигнал, който не води до по-нататъшно разследване или който е неоснователен, ще бъдат незабавно изтрети/унищожени. (6) Субектите, чиито лични данни се обработват във връзка с конкретен сигнал, имат право да упражнят правата си, съобразно приложимото законодателство и вътрешните	Art. 30. (1) Any Personal Data processing, including exchange or transmission of Personal Data by the competent authorities, shall take place in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680 and where such transmission involves the institutions, bodies, offices or agencies of the European Union – in accordance with Regulation (EU) 2018/1725, as well as in accordance with the Personal Data Protection Act. (2) The Company shall implement appropriate technical and organizational measures in accordance with its internal regulations and procedures and the applicable national and European legislation that ensure the lawful processing of Personal Data when receiving and reviewing reports according to the procedure described in this Policy. (3) Any processing, including the transmission of Personal Data, shall be only done to the extent necessary for the purpose of investigating the report and in accordance with Regulation (EU) 2016/679 and the Personal Data Protection Act. (4) No Personal Data that are evidently irrelevant to the review of the particular report shall be collected or, if such data are accidentally collected, they shall be deleted. (5) Personal Data processed in relation to a report that does not give rise to any subsequent investigation or which is ungrounded will be immediately deleted/destroyed. (6) Data subjects whose data are processed in relation to a specific report are entitled to exercise their rights under the applicable legislation and the internal regulation of the Company related to its application.



за Дружеството нормативни документи по прилагането му. (7) Документите по сигналите, кореспонденцията във връзка с подаден сигнал, както и доказателствата към него, се съхраняват за срок, определен в нормативните актове, включително ЗЗЛПСПОИН и Наредба № 1 от 27 юли 2023г. за воденето на регистъра на сигналите. (8) След изтичане на законовите срокове и ако няма правно основание за продължаване на съхранението, документите се архивират и унищожават по сигурен начин.	(7) Documents related to reports, correspondence concerning a submitted report, as well as the evidence accompanying it, shall be retained for the period prescribed by the applicable law, including the LPPWRPDIB and Ordinance No. 1 of 27 July 2023 on the maintenance of the register of reports. (8) Upon expiration of the statutory retention periods, and if there is no legal basis for continued storage, the documents shall be archived and securely destroyed
Чл. 31. (1) За неуредените в настоящите Правила въпроси, се прилагат разпоредбите на ЗЗЛПСПОИН, Наредба № 1 от 27 юли 2023г. за воденето на регистъра на сигналите по чл. 18 от ЗЗЛПСПОИН и за препращане на вътрешни сигнали към Комисията за защита на лични данни, Методическите указания на КЗЛД по прилагането на ЗЗЛПСПОИН и други относими актове. Всички текстове на тези Правила, които противоречат или биха могли да се тълкуват в противоречие с действащото българско или европейско законодателство, се заменят по право със съответните нормативни разпоредби. (2) Прилагането на тези Правила при никакви обстоятелства не може да представлява основание за намаляване на нивото на защита и ако в законодателство е предвидена по-висока защита, то ще има превес.	Art. 31. (1) Any matters that have not been considered in this Policy shall be handled in accordance with the provisions of LPPWRPDIB, Regulation No. 1 of 27 July 2023 on report record-keeping under Art. 18 of LPPWRPDIB and for forwarding internal reports to the Commission for Personal Data Protection, the Methodological Guidelines of CPDP on the application of LPPWRPDIB and any other relevant legislation. All provisions in this Policy that are in conflict or could be interpreted in conflict with the Bulgarian or European legislation that is currently in force shall be replaced by the relevant regulatory provisions by law. (2) Under no circumstances may the application of this Policy constitute any ground for decreasing the level of protection and any stricter protection envisaged in the legislation shall prevail.
Чл. 32. (1) Всички въпроси относно Правилата и нейните принципи могат да бъдат насочвани към Отговорното лице на: Email: whistleblower@intermedica.eu Телефон: 0886 43 73 83	Art. 32. (1) Any questions about this Policy and its principles can be referred to the Responsible Person at: Email: whistleblower@intermedica.eu Telephone: 0886 43 73 83
IX. ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ	IX. TRANSITIONAL AND FINAL PROVISIONS
§ 1. Настоящите Правила са утвърдени със заповед на представляващия Дружеството на 15.12.2023г., влизат в сила от същата дата и са изменени и допълнени на 01.02.2024г. и 30.03.2026.	§ 1. This Policy have been approved with an order of the Company representative of 15.12.2023 and shall enter into force on the same date. These Policy have been amended or supplemented on 01.02.2024 and 30.03.2026.



§ 2. Изменение и допълнение на настоящите Правила се извършват само писмено по реда на тяхното приемане.	§ 2. Any amendment of or supplement to this Policy shall be only made in writing in the order of its adoption.
§ 3. Най-малко веднъж на 3 (три) години Правилата се преразглеждат, извършва се анализ на практиката по ЗЗЛПСПОИН и при необходимост, те се актуализират.	§ 3. The Policy shall be subject to review, analysis of the cases under LPPWRPDIB and, if necessary, updates, at least once every 3 (three) years.
§ 4. Неразделна част от настоящите Правила са следните приложения: Приложение № 1 Формуляр за регистриране на сигнал Приложение № 2 Регистър на сигналите	§ 4. The following annexes constitute an integral part of this Policy: Annex No. 1 Report Recording Form Annex No. 2 Record of Reports

Потвърждение за запознаване с политиката