



*Вътрешни правила  
за функциониране на вътрешния канал за подаване на  
сигнали за нарушения*

**Прилагачи се в:  
“АК Електрик” АД**

*Internal rules  
on the functioning of the Internal channel for reporting  
breaches*

*Applicable in AQ Electric AD*

## Съдържание / Table of Contents

<b>I. ОБЩИ ПОЛОЖЕНИЯ GENERAL PROVISIONS</b> .....	3
<b>II. ЗАЩИТА НА СИГНАЛИЗИРАЩИТЕ ЛИЦА PROTECTION OF REPORTING PERSONS</b> .....	5
<b>III. СЛУЖИТЕЛ, ОТГОВАРЯЩ ЗА РАЗГЛЕЖДАНЕТО НА СИГНАЛИ OFFICER RESPONSIBLE FOR HANDLING REPORTS</b> .....	6
<b>IV. РЕД ЗА РАЗГЛЕЖДАНЕ НА СИГНАЛИ PROCEDURE FOR HANDLING REPORTS</b> ..	9
ПОДАВАНЕ И РЕГИСТРИРАНЕ НА СИГНАЛИТЕ SUBMISSION AND REGISTRATION OF REPORTS .....	9
ПРЕКРАТЯВАНЕ НА ПРОВЕРКАТА TERMINATION OF PROCEEDINGS .....	18
<b>V. РЕГИСТЪР НА СИГНАЛИТЕ И МЕРКИ ЗА СИГУРНОСТ REGISTER OF REPORTS. SECURITY MEASURES</b> .....	18
<b>VI. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ ADDITIONAL PROVISIONS</b> .....	21

## I. ОБЩИ ПОЛОЖЕНИЯ

**Чл.1.** Настоящите Вътрешни правила уреждат създаването на канал за вътрешно сигнализиране за нарушения и регламентират реда и условията за подаване на сигнали или оповестяване на информация в организацията на:

„АК Електрик“ АД, ЕИК 113561397, седалище и адрес на управление в гр. Радомир, ул. „Райко Даскалов“ № 68, представлявано от Изпълнителния Директор – **Емил Николов**, (наричано по-долу „Дружеството“), както и вътрешния канал за подаване на сигнали в Дружеството.

**Чл.2.** (1) Вътрешните правила регламентират реда за подаване на сигналите в организацията на Дружеството, функциите на служителя, отговарящ за разглеждането на сигналите, реда за разглеждането им от Дружеството, както и реда и условията за поддържане, съхраняване и осъществяване на достъп до Регистъра на сигналите.

(2) Настоящите Вътрешни правила се прилагат по отношение на сигнали или публично оповестяване на информация за:

1. нарушения на българското законодателство или на посочените в приложението към Закона за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения („ЗЗЛПСПОИН“/“Закона/ът“) актове на Европейския съюз в областта на:

- 1.1. обществените поръчки;
- 1.2. финансовите услуги, продукти и пазари и предотвратяването на изпирането на пари и финансирането на тероризма;
- 1.3. безопасността и съответствието на продуктите;
- 1.4. безопасността на транспорта;
- 1.5. опазването на околната среда радиационната защита и ядрената безопасност;

## I. GENERAL PROVISIONS

**Art.1.** These Internal Rules govern the establishment of a channel for internal reporting of violations and regulate the terms and conditions for reporting or disclosing information in the organization of:

**AQ Electric AD**, UIC: 113561397, registered office and registered address at 68 Rayko Daskalov str., Radomir, represented by the Executive Director – **Emil Nikolov** (hereinafter referred to as the "Company") as well as the internal reporting channel in the Company.

**Art.2.** (1) The internal rules regulate the procedure for submitting reports in the organization of the Company, the functions of the employee responsible for following-up on the reports, the procedure for their consideration by the Company, as well as the terms and conditions for maintaining, storing and accessing the Register of Reports.

(2) These Internal Rules apply to reports or public disclosure of:

1. Breaches of Bulgarian legislation or of the European Union Acts specified in the Annexes to the Protection of Persons Who Report or Publicly Disclose Information on Breaches Act (the "Act") in the fields of:

- 1.1. Public procurement;
- 1.2. financial services, products and markets and the prevention of money laundering and terrorist financing;
- 1.3. safety and conformity of products;
- 1.4. Safety of transportation
- 1.5. Environmental protection, radiation protection and nuclear safety;

- |  |  |
|--|--|
| <p>1.6. безопасността на храните и фуражите, здравето на животните и хуманното отношение към тях;</p> <p>1.7. общественото здраве;</p> <p>1.8. защитата на потребителите;</p> <p>1.9. защитата на неприкосновеността на личния живот и личните данни;</p> <p>1.10. сигурността на мрежите и информационните системи;</p> <p>2. нарушения на българското законодателство в областта на:</p> <p>2.1. правилата за заплащане на дължими публични държавни и общински вземания;</p> <p>2.2. трудовото законодателство;</p> <p>2.3. законодателството, свързано с изпълнението на държавна служба.</p> <p>3. нарушения, които засягат финансовите интереси на Европейския съюз по смисъла на чл. 325 и нарушения на правилата на вътрешния пазар по смисъла на чл. 26, параграф 2 от Договора за функционирането на Европейския съюз и допълнително уточнени в съответните мерки на Съюза;</p> <p>4. 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;</p> <p>5. извършено престъпление от общ характер, за което лицето е узнало във връзка с извършване на своята работа или при изпълнение на служебните си задължения.</p> <p>(3) Дружеството предприема необходимите мерки, предвидени в настоящите Вътрешни правила, за да поощрява сигнализирането чрез канала за вътрешно подаване на сигнали.</p> | <p>1.6. food and feed safety, animal health and welfare;</p> <p>1.7. Public health</p> <p>1.8. Customer protection</p> <p>1.9. the protection of privacy and personal data</p> <p>1.10. the security of network and information systems;</p> <p>2. Breaches of Bulgarian legislation in the field of:</p> <p>2.1. the rules for payment of public state and municipal receivables;</p> <p>2.2. Labour legislation</p> <p>2.3. legislation relating to the performance of a civil service.</p> <p>3. Breaches affecting the financial interests of the European Union within the meaning of art. 325 and infringements of the rules of the internal market within the meaning of art. 26, par. 2 of the Treaty on the Functioning of the European Union and further specified in the relevant Union measures;</p> <p>4. breaches relating to cross-border tax schemes the purpose of which is to obtain a tax advantage which is contrary to the object or purpose of the applicable corporate tax law;</p> <p>5. a crime which has been committed, of which the person has become aware in connection with the performance of his work or in the performance of his duties.</p> <p>(3) The Company shall take the necessary measures provided for in these Internal Rules to encourage reporting through the internal reporting channel.</p> |
|--|--|

(4) С настоящите вътрешни правила се създава канал за вътрешно подаване на сигнал за нарушения, който отговаря на следните изисквания:

1. управлява се по начин, който гарантира пълнотата, целостта и поверителността на информацията и възпрепятства достъпа на неоправомощени лица до тази информация;

2. дава възможност за съхранение на записана на траен носител информация за нуждите на проверката по сигнала и за по-нататъшни разследвания.

## II. ЗАЩИТА НА СИГНАЛИЗИРАЩИТЕ ЛИЦА

**Чл.3.** (1) Защита по ЗЗЛПСПОИН и тези Правила се предоставя на:

1. Физическо лице, което подава сигнал или публично оповестява информация за нарушения, станала му известна в работен контекст, при или по повод изпълнение на трудовите или служебните му задължения или е получена по време на процеса на подбор или други преддоговорни отношения („сигнализиращо лице“);

2. Лица, които помагат на сигнализиращото лице в процеса на подаването на сигнал, и чиято помощ следва да е поверителна;

3. Лица, които са свързани посредством работата си или са роднини на сигнализиращото лице, и които могат да станат обект на ответни действия във връзка със сигнала.

(2) Сигнализиращото лице по ал. 1, т. 1 може да бъде както служител на Дружеството, така и бивш служител, както и лице, което полага труд без трудов договор, стажант, изпълнител, подизпълнител или доставчик на Дружеството, външен консултант, едноличен собственик или акционер в Дружеството, както

(4) These internal rules establish a channel for internal reporting of breaches that meets the following requirements:

1. it is managed in such a way as to ensure the completeness, integrity and confidentiality of the information and to prevent unauthorised persons from accessing that information;

2. enables the storage of information recorded on a durable medium for the purpose of following-up on the report and for further investigations.

## II. PROTECTION OF REPORTING PERSONS

**Art.3.** (1) The following persons have the right to obtain Protection under the Act and these Rules:

1. A natural person who reports or publicly discloses information about breaches that has become known to him in a working context, during or in connection with the performance of his or her employment or official duties, or is obtained during the selection process or other pre-contractual relationship ('reporting person');

2. Persons who assist the reporting person in the reporting process and whose assistance should be confidential;

3. Persons who are connected through their work or are related to the reporting person and who may be the subject of retaliation in connection with the report.

(2) The reporting person under par. 1, item 1 may be an employee of the Company, a former employee, as well as a person who performs work without an employment contract, a trainee, contractor, subcontractor or supplier of the Company, an external consultant or shareholder in the Company, as well as any other reporting person

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

(3) Лицата по ал. 1 са защитени лица и служителите, които разглеждат сигнала в организацията на Дружеството, нямат право да оповестяват самоличността им, с изключение на случаите, когато е необходимо сигналът да достигне до конкретната институция, отговаряща за предприемане на законовите действия и наказване на нарушителите.

**Чл.4.** (1) Лице, подаващо сигнал за нарушения чрез вътрешен или външен канал, има право на защита, когато са изпълнени едновременно следните условия:

1. е имало основателна причина да счита, че подадената информация за нарушението в сигнала е била вярна към момента на подаването и че тази информация попада в обхвата на Закона; и

2. е подало сигнал за нарушение при условията и по реда на ЗЗЛПСПОИН и тези Правила.

(2) При наличие на условията по-горе право на защита има и лицето, което подава сигнал за нарушение до институции, органи, служби или агенции на Европейския съюз.

**Чл.5.** Спрямо лицата с право на защита се забранява всяка форма на ответни действия, имащи характера на репресия и поставящи ги в неблагоприятно положение, както и заплахи или опити за такива действия.

### III. СЛУЖИТЕЛ, ОТГОВАРЯЩ ЗА РАЗГЛЕЖДАНЕТО НА СИГНАЛИ

**Чл.6.** (1) Ръководството на Дружеството определя със заповед един или повече служители, които да отговарят за разглеждането на сигналите, подадени по реда на настоящите Вътрешни правила (оттук

who reports a violation which has become known to him or her in a working context.

(3) The persons under par. 1 are protected persons and the employees who consider the report in the Company's organization have no right to disclose their identity, except for the cases when it is necessary for the report to reach the specific authority responsible for taking legal action and sanctioning the offenders.

**Art.4.** (1) A person reporting breaches through an internal or external channel shall be entitled to protection where the following conditions are simultaneously met:

1. had reasonable cause to believe that the information submitted about the breach in the report was correct at the time of its submission and that such information falls within the scope of the Act; and

2. has reported a violation under the terms and conditions of the Act and these Rules.

(2) Subject to the conditions above, the right to protection is also available to persons reporting to institutions, bodies, offices or agencies of the European Union.

**Art.5.** Any form of retaliation which can be categorized as repression against Persons entitled to protection and putting them at a disadvantage is prohibited, as are all threats or attempts at such acts.

### III. OFFICER RESPONSIBLE FOR HANDLING REPORTS

**Art.6.** (1) The management of the Company shall appoint by resolution one or more employees to be responsible for reviewing the signals submitted under these Internal Rules (hereinafter the

нататък служителят/служителите общо ще се наричат „Служител по ЗЗЛПСПОИН“).

(2) Дейността по разглеждане на получените сигнали се състои от две самостоятелни функции, както следва:

1. приемане и регистриране на подадените сигнали; и
2. разглеждане на сигналите.

**Чл.7.** При осъществяване на функциите си, Служителят по ЗЗЛПСПОИН е длъжен да:

1. Получава и администрира сигналите и потвърждава получаването им в предвидените срокове;
2. Гарантира, че самоличността на сигнализиращото лице и другите лица, посочени в сигнала, ще бъде надлежно защитена;
3. Прилага подходящи мерки за защита на информацията, съдържаща се в сигнала и за ограничаване достъпа до него;
4. Поддържа връзка със сигнализиращото лице, предоставя информация за извършените действия по сигнала, и при необходимост изисква допълнителни сведения от сигнализиращото лице;
5. Предоставя на лицата, желаещи да подадат сигнал, ясна и достъпна информация за възможностите за външно подаване на сигнал до централния орган за външно подаване на сигнали (Комисията за защита на личните данни или „КЗЛД“) или друг компетентен орган когато е необходимо;
6. Поддържа Регистъра на сигналите съобразно реда и условията на настоящите Правила и модела на регистър, публикуван от КЗЛД;
7. Дава възможност на лицето, срещу което е подаден сигнала или засегнатото лице да даде обяснения, да представи или поиска допълнителни доказателства и му дава

employee/employees will be collectively referred to as the "Responsible Officer").

(2) Investigation of reports consists of the following separate functions:

1. receiving and registering the submitted reports; and
2. consideration of reports.

**Art.7.** In carrying out his/her functions, the Responsible Officer shall:

1. Receive and administer reports and acknowledges their receipt within the prescribed deadlines;
2. Ensure that the identity of the reporting person and other persons referred to in the report is properly protected;
3. Implement appropriate measures to protect the information contained in the report and to restrict access to it;
4. Liaise with the reporting person, provide information on the activities taken in investigating the report and, if necessary, request further information from the reporting person;
5. Provide persons wishing to submit a report with clear and accessible information about the possibilities for external reporting to the central authority for external reporting (the Commission for Personal Data Protection or CPDP) or another competent authority where necessary;
6. Maintain the Register of Reports in accordance with the terms and conditions of these Rules and the model register published by the CPDP;
7. Enable the person against whom the report was submitted or the person concerned in the report to provide explanations, to present or request additional evidence and allow them the



възможност да направи възражения по изложените в сигнала твърдения;

8. В случай, че фактите, посочени в сигнала бъдат потвърдени, извършва необходимите последващи действия съгласно ЗЗЛПСПОИН и настоящите Правила.

**Чл.8.** Функцията по приемане и регистриране на сигнала включва действията по приемане на сигнала и неговото завеждане с входящ номер от информационната система за документооборота на Дружеството (или с друг аналогичен идентификатор, съдържащ пореден номер и дата на подаване на сигнала). Функцията по приемане и регистриране на сигнали може да бъде възложена на външно за Дружеството лице със заповед на ръководния орган.

**Чл.9.** (1) Функцията по разглеждане на сигнала включва последващите действия по проверката му, като преценката за неговата допустимост и достоверност, информирането на сигнализиращото лице и засегнатите от сигнала лица, извършване на вътрешна проверка, препращането му на КЗЛД, както и изготвянето на доклад за извършените действия.

(2) При изпълнение на задачите по разглеждане на сигнали, отговорният Служител по ЗЗЛПСПОИН е функционално независим и не може да получава указания или нареждания във връзка с разглеждането на сигнала.

**Чл.10.** (1) За разглеждане на сигнали, подадени срещу Служителя по ЗЗЛПСПОИН, ръководството на Дружеството може да определи резервен служител (служители).

(2) На Служителя по ЗЗЛПСПОИН се провежда инструктаж от компетентни лица в областта на законодателството, свързано със защита на лицата, подаващи сигнали или публично оповестяващи информация за

opportunity to raise objections to the allegations made in the report;

8. In the event that the facts stated in the alert are confirmed, perform the necessary follow-up actions under the Act and these Rules.

**Art.8.** The function of receiving and registering the report includes the actions of receiving the report and its filing with a serial number from the Company's document filing system (or with another similar identifier containing a serial number and date of submission of the report). The function of receiving and registering reports can be assigned to a third-party provider outside the structure of the Company with a resolution of its management.

**Art.9.** (1) The function of handling the report shall include the follow-up actions for its review, such as the assessment of its admissibility and reliability, the informing of the reporting person and the persons affected by the report, carrying out an internal check, its forwarding to the CPDP, as well as the drafting of a report on the actions carried out.

(2) In performing the tasks of reviewing report, the Responsible Officer shall be functionally independent and shall not be subject instructions or orders in connection with the consideration of the report.

**Art.10.**(1) The management of the Company may appoint a reserve employee (or employees) for the consideration of reports submitted against the Responsible Officer.

(2) The Responsible Officer shall undergo training by competent persons in the field of legislation related to the protection of whistleblowers. They are instructed and trained in advance both to safeguard the rights of the subjects



нарушения. Същите са предварително инструктирани и обучени както да спазват правата на субектите, така и да пазят самоличността на всички засегнати лица и поверителността на информацията от вписването ѝ в регистъра на сигналите до етапа на изготвянето на индивидуален доклад за действията по разглеждане на сигнала.

#### IV. РЕД ЗА РАЗГЛЕЖДАНЕ НА СИГНАЛИ

##### ПОДАВАНЕ И РЕГИСТРИРАНЕ НА СИГНАЛИТЕ

**Чл.11.** (1) Вътрешното подаване на сигнали за нарушения следва реда на настоящите Вътрешни правила, които са базирани на принципите за поверителност на информацията и защита на самоличността, както на лицата, подаващи сигналите, така и на засегнатите от сигнала лица.

(2) Сигналите за нарушения могат да се подават писмено или устно, по един от следните начини:

1. чрез определената електронна поща на Дружеството за подаване на сигнали – [yankov@ynglegal.com](mailto:yankov@ynglegal.com), достъп до която имат само лицето, натоварено с осъществяването на функцията по приемане и регистриране на сигналите;

2. чрез попълване на формуляра за вътрешно подаване на сигнал и подаването му до лицето, отговарящо за приемането и регистрирането на сигналите;

3. устно по телефона, на специално определената за целта телефонна линия – 0888300226;

4. устно, чрез лична среща, уговорена между лицето, желаещо да подаде сигнал, и Служителя по ЗЗЛПСПОИН.

(3) За подаването на писмени сигнали, сигнализиращите лица ползват одобрения от КЗЛД формуляр, разпечатан и поставен на достъпно място в деловодството на

and to protect the identity of all affected persons and the confidentiality of information from its entry in the Register of reports to the stage of preparing an individual report on the actions for reviewing the report.

#### IV. PROCEDURE FOR HANDLING REPORTS

##### SUBMISSION AND REGISTRATION OF REPORTS

**Art.11.**(1) Internal reporting of breaches follows the present Internal Rules, which are based on the principles of confidentiality of information and identity protection, for both reporting persons and persons affected by the report.

(2) Reports of breaches may be submitted in writing or orally in one of the following ways:

1. via the designated e-mail address of the Company for reporting breaches which is accessed only by the person appointed to perform the function of receiving and registering reports – [yankov@ynglegal.com](mailto:yankov@ynglegal.com);

2. by filling in the form for internal reporting and submitting it to the person responsible for receiving and registering the reports;

3. by telephone, on the dedicated telephone line — 0888300226;

4. through a personal meeting agreed between the person wishing to report and the Responsible Officer.

(3) For the submission of written reports, the reporting persons use the form approved by the CPDP, printed and placed in an accessible place in the office of the Company and/or on its website. If

Дружеството и/или на неговата интернет страница. Ако сигнализиращо лице подаде сигнал във форма, различна от утвърдения от КЗЛД формуляр, Служителят по ЗЗЛПСПОИН прилага този сигнал към формуляра и попълва формуляра с наличната в сигнала информация.

(4) Устният сигнал се документира чрез попълване на формуляр от Служителя по ЗЗЛПСПОИН, който предлага на подаващия сигнала да го подпише при желание от негова страна.

**Чл.12.** (1) Сигналът следва да съдържа най-малко следната информация:

1. трите имена, адрес и телефон на подателя, както и електронен адрес, ако има такъв;
2. имената на лицето, срещу което се подава сигналът, и неговата месторабота, ако сигналът се подава срещу конкретни лица и те са известни;
3. конкретни данни за нарушение или за реална опасност такова да бъде извършено, място и период на извършване на нарушението, ако такова е извършено, описание на деянието или обстановката и други обстоятелства, доколкото такива са известни на сигнализиращото лице;
4. дата на подаване на сигнала;
5. подпис, електронен подпис или друга идентификация на подателя.

(2) 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 за лица, които биха могли да потвърдят съобщените данни или да предоставят допълнителна информация.

(3) Ако сигналът не съдържа минимално установената информация, същият се счита за нередовен, и на сигнализиращото лице се изпращат указания за предоставяне на допълнителна информация с цел отстраняване на нередовностите в срок до 7 дни с указания, че непредоставянето им ще предизвика

a reporting person submits a report in a form different from the form approved by CPDP, the Responsible Officer attaches this report to the form and fills in the form with the information available in the report.

(4) Oral reports shall be documented by filling in a form by the Responsible Officer, who suggests the reporting person sign the report if he or she so wishes.

**Art.12.**(1) The report should contain at least the following information:

1. Full name, address and phone number of the reporting person, as well as an email address if applicable;
2. The names of the person against whom the report is made and his/her place of work, if the alert is issued against specific;
3. specific information of a breach or of an actual danger of such breach occurring, the place and period of the breach, if one has occurred, a description of the act or situation and other circumstances, to the extent known to the reporting person;
4. Data of filing the report
5. Signature, e-signature or other identification of the reporting person

(2) The report may be accompanied by any kind of information supporting the allegations made therein and/or reference to documents, including the indication of data on persons who could confirm the data communicated or provide additional information.

(3) If the report does not contain the minimum established information, it shall be considered irregular, and instructions for the provision of additional information shall be sent to the reporting person in order to remedy the irregularities within 7 days, with instructions that failure to provide them will trigger the termination of the reporting proceedings.

прекръпяване на производството по разглеждане на сигнала.

(4) 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 набеждаване.

(5) При неподаването на допълнителната информация в срок, сигналът се приема за нередовен и не се разглежда, за което се уведомява сигнализиращото лице, и на същото се посочва, че има право да подаде сигнала повторно. Приемането на сигнала за нередовен и прекръпяване на производството по неговото разглеждане не освобождава Служителя по ЗЗЛПСПОИН от задължението му да не разкрива самоличността на сигнализиращото лице.

**Чл.13.** (1) Служителят по ЗЗЛПСПОИН приема подадения сигнал, като при необходимост попълва утвърдения от КЗЛД формуляр за вътрешно сигнализиране, в случаите когато сигналът е подаден писмено в свободен текст или лицето е сигнализирано устно.

(2) В случай че сигнал за нарушения се получи по начин, различен от този, регламентиран в чл. 11, ал. 2 или от служител, различен от Служителя по ЗЗЛПСПОИН или лицето, изпълняващо функцията по приемане и регистриране на сигналите, на получилия го служител се забранява да разкрива всякаква информация, чрез която би могло да се установи самоличността на сигнализиращото или засегнатото лице. Сигналът се препраща незабавно, без изменения, на Служителя по ЗЗЛПСПОИН за регистрирането му.

(3) След приемането му, сигналът се завежда с входящ номер от вътрешната деловодна система на Дружеството или друг сходен идентификационен номер, съдържащ датата на подаване на сигнала.

(4) След постъпване на сигнала се извършва първоначален формален преглед за редовност и допустимост на сигнала, по-конкретно дали

(4) Reports that contain manifestly false or misleading statements of fact shall be returned with an instruction to the sender to correct the allegations and the responsibility he bears for false accusations.

(5) In case of failure to submit the additional information in time, the report shall be considered invalid and shall not be considered, for which the reporting person shall be notified, and the latter shall be informed that he or she has the right to file a new report. The deeming of the report as invalid and termination of the proceedings for its consideration does not relieve the Responsible Officer from his/her obligation not to disclose the identity of the reporting person.

**Art.13.**(1) The Responsible Officer receives the filed report and if necessary, fills the internal reporting form approved by CPDP when the report is filed in writing as a free text or orally.

(2) Where a report is received in a different from the specified in Art. 11, para. 2 way or by a staff member other than the Responsible Officer or the person responsible for receiving and registering the reports, the staff member who receives it is prohibited from disclosing any information that might identify the reporting person or the person concerned. They must promptly forward the report without modification to the Responsible Officer for its registration.

(3) After the admission of the report, it is filed with a serial number from the internal filing system of the Company or another similar identification number, containing the date the report is filed.

(4) After receiving the report, an initial check is performed if the report meets the initial requirements and is admissible, namely: if it falls

сигналът попада в приложното поле на Закона. Не се регистрират с УИН сигнали, от първоначалния преглед на които е очевидно, че касаят оплакване (жалби или сигнали) за нередности или неудовлетвореност на клиенти/потребители на съответните професионални или административни услуги на Дружеството. Такива сигнали не попадат в обхвата на ЗЗЛПСПОИН и не се разглеждат по неговите ред и условия.

(5) Служителят по ЗЗЛПСПОИН генерира Уникален идентификационен номер (УИН), предоставен от КЗЛД. УИН се генерира чрез интернет страницата на КЗЛД, след което се вписва в съответния формуляр за подадения сигнал.

(6) УИН се генерира включително за сигнали:

1. отнасящи се до нарушения, извършени преди повече от две години;

2. чието съдържание не дава основание да се приемат за правдоподобни;

3. съдържащи очевидно неверни или заблуждаващи твърдения за факти;

4. за нарушения, подлежащи на докладване по специална нормативна уредба;

5. за нарушения, които вече са констатирани от вътрешно звено на Дружеството (напр. вътрешен одит или инспекторат), независимо дали са предприети действия по отстраняването им;

6. които са били подадени анонимно или анонимно е била оповестена информация за нарушения, но техните автори впоследствие са били идентифицирани и са станали обект на репресивни ответни действия.

**Чл.14.** (1) Анонимни сигнали не се разглеждат, за такива сигнали не се генерира УИН и не се регистрират в регистъра по закона. Анонимен сигнал може да бъде разгледан по ред и условия

within the scope of the Act. No UIN shall be generated for reports, from the initial review of which it is obvious that they concern a complaint (complaints or signals) about irregularities or dissatisfaction of clients / users of the relevant professional or administrative services of the Company. Such signals do not fall within the scope of the Act and are not considered under its terms and conditions.

(5) The Responsible Officer generates a Unique Identification Number (UIN) provided by the CPDP. UIN is generated through the CPDP's website, after which it is entered in the relevant reporting form.

(6) UIN is generated including for reports:

1. pertaining to breaches committed more than two years prior to the report;

2. the content of which does not justify being considered plausible;

3. containing manifestly false or misleading statements of fact;

4. for breaches subject to reporting under special regulations;

5. for breaches that have already been discovered by an internal unit of the Company (e.g. internal audit or inspectorate), regardless of whether actions have been taken to eliminate them;

6. were submitted anonymously or information about breaches was disclosed anonymously, but their authors were subsequently identified and became the subject of repressive retaliation.

**Art.14.**(1) Anonymous reports shall not be considered, for such reports no UIN shall be generated and shall not be registered in the Register. An anonymous report may be considered

извън тези по закона, ако правната уредба, приложима към дейността на Дружеството или неговите вътрешни актове, налагат или допускат това. В тези случаи анонимният сигнал може да се разглежда за цели, различни от целите на ЗЗЛПСПОИН и да се води в отделен регистър.

(2) Когато лице е подало анонимен сигнал не по реда на ЗЗЛПСПОИН или публично, но анонимно, е оповестило информация за нарушения, но впоследствие е било идентифицирано и е станало обект на ответни действия, това лице има право на защита, когато са налице останалите условия за защита по Закона. Преценката за това е от компетентността на Служителя по ЗЗЛПСПОИН, който прави проверка, като следва:

1. дали лицето, подало анонимен сигнал или публично оповестяващо информация, е имало основателна причина да счита, че подадената информация за нарушението в сигнала е била вярна към момента на подаването ѝ и че тази информация попада в обхвата на чл. 3 от Закона;

2. дали лицето, публично оповестяващо информация е подало сигнал при условията и по реда на ЗЗЛПСПОИН, но сигнала не са били предприети съответни действия в сроковете, предвидени по раздели I и II на глава втора на закона;

3. дали лицето, публично оповестяващо информация, има основания да смята, че нарушението може да представлява непосредствена или явна опасност за обществен интерес или съществува риск от щети, които не могат да бъдат отстранени;

4. дали в случай на външно подаване на сигнал 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 компетентния орган и

under terms and conditions outside those of the Act, if the legal framework applicable to the Company's activity or its internal acts requires or allows this. In these cases, the anonymous report may be considered for purposes other than the purposes of the Act and kept in a separate register.

(2) When a person has submitted an anonymous report not under the Act, or has publicly, but anonymously, disclosed information about breaches, but has subsequently been identified and has become the subject of retaliatory actions, that person has the right to protection when the other conditions for protection under the Act are met. The assessment of this is within the competence of the Responsible Officer, who conducts an inspection as to the following:

1. whether the person submitting an anonymous report or publicly disclosing information had reasonable grounds to believe that the information submitted about the breach in the report was correct at the time of its submission and that such information falls within the scope of art. 3 of the Act;

2. whether the person publicly disclosing information has filed a report under the terms and conditions of the Act, but no appropriate action has been taken on the report within the time limits provided for in Sections I and II of Chapter Two of the Act;

3. whether the person publicly disclosing information has reason to believe that the breach may present an immediate or manifest danger to the public interest or there is a risk of damage that cannot be remedied;

4. whether, in the case of external reporting, there is a risk of retaliation or is likely that the breach will not be effectively addressed due to the risk of concealment or destruction of evidence, suspicion of collusion between the competent authority and the perpetrator of the breach, or of the authority's complicity in the



извършителя на нарушението, или за съучастие на органа в нарушението, както и поради други специфични конкретни обстоятелства по случая.

(3) При наличието на горепосочените условия за защита на лицата Служителят по ЗЗЛПСПОИН попълва формуляр за регистриране на сигнали, генерира УИН и го вписва във формуляра, като завежда така подадения сигнал или публично оповестена информация със собствен входящ номер от информационната система за документооборота или с друг идентификатор, съдържащ пореден номер и дата на подаване на анонимния сигнал/дата на публично оповестяване на информацията за нарушения.

**Чл.15.** В срок от 7 дни, считано от получаването на сигнала, Служителят по ЗЗЛПСПОИН, потвърждава получаването на сигнала като уведомява сигнализиращото лице за генерирания УИН на неговия сигнал и за собствения входящ номер от деловодството на дружеството чрез уведомление, а при устно подаден сигнал, сигнализиращото лице се уведомява по телефон или лично и му се указва да предостави контакт, за да може да му се изпрати писменото уведомление.

#### РАЗГЛЕЖДАНЕ НА СИГНАЛИТЕ

**Чл.16.** (1) Когато сигналът съдържа минимално установената информация и е редовен, същият подлежи на разглеждане относно неговата достоверност.

(2) При условията и по реда на ЗЗЛПСПОИН и настоящите правила се разглеждат единствено сигнали, които попадат в обхвата на чл. 3 от ЗЗЛПСПОИН, не са изтекли две години от извършването на твърдяното нарушение/нарушения, и са подадени от някое от лицата по чл. 3 от Правилата.

(3) Служителят по ЗЗЛПСПОИН извършва преценка дали нарушението, за което се отнася сигнала, попада в обхвата на изключенията от приложното поле, предвидени в чл. 4 от Закона;

breach, as well as other specific circumstances of the case.

(3) In the presence of the above conditions for the protection of individuals, the Responsible Officer fills in a signal registration form, generates a UIN and enters it in the form, filing the submitted report or publicly disclosed information with its own reference number from the document filing system or with another identifier containing a serial number and date of submission of the anonymous report/date of public disclosure of information about breaches.

**Art.15.** Within 7 days from the receipt of the report, the Responsible Officer confirms the receipt of the report by notifying the reporting person of the generated UIN for his report and of the serial number from the Company's filing system by means of a notification form, and in case of an oral signal, the reporting person shall be notified by phone or in person and instructed to provide contact information, so that the written notification can be sent to him.

#### HANDLING OF REPORTS

**Art.16.**(1) Where the reports contains the minimum information and is valid, it shall be subject to consideration as to its reliability.

(2) Under the terms and conditions of the Act and these rules, only reports that fall within the scope of Art. 3 of the Act, concern alleged breach/breaches committed less than two years prior, and have been filed by any of the persons under art. 3 of the rules, shall be considered.

(3) The Responsible Officer shall assess whether the reported breach falls within the exceptions to its scope provided for in art. 4 of the Act;

(4) Разглеждането на постъпили множество сигнали за нарушения се приоритизира, съгласно следните критерии, изложени в низходящ ред по степен на значимост:

1. вид на нарушението (данни за престъпление или административно нарушение);
2. размер на предполагаемите преки материални щети от нарушението;
3. размер на предполагаемите непреки материални щети;
4. вид и размер на наказанията, които е възможно да бъдат наложени от компетентните органи за отделните нарушения;
5. извършеното нарушение оказва или би могло да окаже значително и трайно във времето отрицателно въздействие върху обществения интерес;
6. потенциални репутационни щети.

**Чл.17.(1)** Служителят по ЗЗЛПСПОИН проверява за наличието на данни за достоверност (правдоподобност) на сигнала, като за целта:

1. извършва проверка по твърденията за нарушения, изнесени в сигнала;
2. изслушва лицето, срещу което е подаден сигналът или приема писмените му обяснения, както ѝ събира и оценява посочените от него доказателства;
3. предоставя на засегнатото лице всички събрани доказателства и му предоставя възможност да направи възражения по тях в 7-мо дневен срок, при спазване на защитата на сигнализиращото лице;
4. предоставя възможност на засегнатото лице да представи и посочи нови доказателства, които да бъдат събрани в хода на проверката;
5. при необходимост осъществява вътрешна комуникация с други служители или

(4) The consideration of multiple reports for breaches is prioritized according to the following criteria, set out in descending order of importance:

1. type of breach (evidence of a crime or administrative violation);
2. the extent of the alleged direct material damage from the breach;
3. the extent of the alleged indirect material damage;
4. the type and amount of penalties which may be imposed by the competent authorities for individual offences;
5. the breach committed has or could have a significant and lasting negative impact on the public interest;
6. potential reputational damages.

**Art.17.(1)** The Responsible Officer shall inspect for the presence of data supporting the credibility (plausibility) of the report, and for this purpose:

1. carry out an investigation of the allegations of violations brought out in the report;
2. hear the person against whom the report has been issued or accept his or her written explanations, as well as collect and evaluate the evidence indicated by them;
3. provide the person concerned with all evidence collected and give him or her the opportunity to object to it within 7 days, subject to the protection of the reporting person;
4. enable the person concerned to present and identify new evidence to be gathered in the course of the inspection;
5. if necessary, carries out internal communication with other employees or units of



звена на Дружеството, функционално компетентни да извършат тази проверка;

б. поддържа комуникация със сигнализиращото лице с цел изясняване на всички въпроси, предмет на сигнала.

(2) Вътрешната комуникация по ал. 1, т. 5 се осъществява от Служителя по ЗЗЛПСПОИН при наличието на подходящи технически и организационни мерки за защита на самоличността на сигнализиращото лице и на всяко друго лице, посочено в сигнала. При разглеждане на сигнала, Служителят по ЗЗЛПСПОИН може да използва услугите на експерти, консултанти или други лица, външни за структурата на Дружеството. В тези случаи информацията по сигнала се предоставя на третите лица при наличието на задължение на третото лице за поверителност и защита на самоличността на сигнализиращото лице, и на принципа „необходимост да се знае“.

(3) Сигналят се приема за достоверен ако към него са налични толкова и такива данни, които, анализирани в своята съвкупност, да доведат до извода, че има вероятност да е извършено твърдяното нарушение в предметния обхват на Закона.

**Чл.18.**(1) Действията на Служителя по ЗЗЛПСПОИН, се документират със съответните протоколи и писмени документи, които се пазят на хартиен или електронен носител, като имената на подалия сигнала и другите засегнати лица се криптират, анонимизират или заличават по начин, по който да не бъдат разпознати от трети лица.

(2) След извършване на вътрешната проверка и в случай на мотивирано становище (мнение) за достоверност на сигнала, Служителят по ЗЗЛПСПОИН:

1. организира предприемането на последващи действия във връзка със сигнала, като за целта може да изисква съдействието на други лица или звена в структурата на Дружеството;

2. предлага на ръководството на Дружеството предприемане на конкретни

the Company functionally competent to carry out this inspection;

б. maintain communication with the reporting person in order to clarify all issues that are the subject of the report.

(2) Internal communication under para. 1, item 5 shall be carried out by the Responsible Officer in the presence of appropriate technical and organizational measures to protect the identity of the reporting person and any other person specified in the report. When considering the report, the Responsible Officer may use the services of experts, consultants or other persons external to the structure of the Company. In such cases, the information on the report shall be provided to third parties subject to the third party's obligation of confidentiality and protection of the identity of the reporting person and on a strictly need-to-know basis.

(3) The report is considered reliable if there is such data available, which, analyzed in its total, lead to the conclusion that there is a likelihood that the alleged breach within the subject scope of the Act is likely to have occurred.

**Art.18.**(1) The actions of the Responsible Officer shall be documented with the relevant protocols and written documents, which shall be kept on paper or electronic medium, and the names of the reporting person and other affected persons shall be encrypted, anonymized or deleted in a way that they are not recognizable by third parties.

(2) After carrying out an internal inspection and in case of a reasoned opinion for the credibility of the report, the Responsible Officer shall:

1. organize a follow-up of the report, and for this purpose may require the assistance of other persons or units in the structure of the Company;

2. propose to take specific measures to the management of the Company in order to stop or

мерки с цел преустановяване или предотвратяване на нарушението в случаите, когато такова е констатирано или има реална опасност за предстоящото му извършване;

3. насочва сигнализиращото лице към компетентните органи, когато се засягат неговите права;

4. препраща сигнала на органа за външно подаване на сигнали при необходимост от предприемане на действия от негова страна, като за препращането сигнализиращото лице се уведомява предварително. Препращането на вътрешен сигнал към КЗЛД не освобождава отговорния служител по ЗЗЛПСПОИН и всяко друго лице, което е имало достъп до сигнала, от задължението им за защита на самоличността на сигнализиращото лице и на всяко друго лице, посочено в сигнала.

Единен централен орган за външно подаване на сигнали е:

Комисията за защита на личните данни  
Адрес: София 1592, бул. „Проф. Цветан Лазаров” № 2;  
Електронна поща: [whistleblowing@cpdp.bg](mailto:whistleblowing@cpdp.bg)

**Чл.19.**(1) Във всеки етап на образуваното производство, при наличие на достатъчно данни, които да потвърждават изнесените в сигнала факти, Служителят по ЗЗЛПСПОИН може да изготви доклад до ръководството на Дружеството, в който да предложи предприемане на конкретни мерки с цел преустановяване или предотвратяване на нарушението и съответно Дружеството може да предприема действия в рамките на своята компетентност с тази цел.

(2) В срок не по-дълъг от 3 месеца след потвърждаване на получаването на сигнала, Служителят по ЗЗЛПСПОИН изготвя индивидуален доклад, който съдържа накратко информацията от сигнала, предприетите действия, окончателните резултати от проверката по сигнала, които заедно с мотивите

prevent the breach in cases where such has been established or there is a real danger for its forthcoming occurrence;

3. refer the reporting person to the competent authorities where his or her rights are affected;

4. forward the report to the external reporting authority where action is necessary on its part, and notify the reporting person of the referral in advance. The forwarding of an internal report to the CPDP does not relieve the Responsible Officer and any other person who has had access to the report from their obligation to protect the identity of the reporting person and any other person specified in the report.

The single external reporting authority is:

the Commission for Personal Data Protection  
Address: Sofia 1592, bul. "Prof. Tsvetan Lazarov"  
No 2;  
E-mail: [whistleblowing@cpdp.bg](mailto:whistleblowing@cpdp.bg)

**Art.19.**(1) At any stage of the initiated proceedings, if there is sufficient data to confirm the facts presented in the report, the Responsible Officer may prepare a report to the management of the Company recommending specific measures in order to terminate or prevent the breach, and the Company may take action within its competence for this purpose.

(2) Within no longer than 3 months after acknowledging the receipt of the report, the Responsible Officer prepares an individual report, which contains abridged information from the report, the actions taken, the final results of the inspection of the report, which together with the motives it communicates to the reporting person

съобщава на подалия сигнала работник или служител и на засегнатото лице при спазване на задължението за тяхната защита, както и на ръководството на Дружеството.

## ПРЕКРАТЯВАНЕ НА ПРОВЕРКАТА

**Чл.20.** (1) Проверката на сигнала се прекратява в следните случаи:

1. когато нарушението, за което е подаден сигналът, е очевидно маловажно и не налага предприемането на допълнителни последващи действия.

2. по повтарящ се сигнал, който не съдържа нова информация от съществено значение за нарушение, по отношение на което вече има приключила проверка, освен ако нови правни или фактически обстоятелства не дават основание за предприемането на последващи действия.

3. Когато се установят данни за извършено престъпление, сигналът и материалите към него се изпращат незабавно на прокуратурата.

(2) При наличие на някоя от описаните по-горе хипотези, Служителят по ЗЗЛПСПОИН изготвя доклад до ръководството на Дружеството с предложение за прекратяване на проверката и Дружеството определя дали проверката да бъде прекратена. При прекратяване на основание ал. 1, т. 1 и 2 по-горе, Служителят по ЗЗЛПСПОИН указва на сигнализиращото лице, че може да подаде сигнал до КЗЛД като национален орган за външно подаване на сигнали.

## V. РЕГИСТЪР НА СИГНАЛИТЕ И МЕРКИ ЗА СИГУРНОСТ

**Чл.21.**(1) Сигналите се документират в Регистъра на сигналите за нарушения, който се води и поддържа на траен носител от Служителя по ЗЗЛПСПОИН. Достъп до регистъра имат само Служителят по

and the affected person, in compliance with the obligation for their protection, as well as to the management of the Company.

## TERMINATION OF THE INVESTIGATION

**Art.20.**(1) The investigation into the report shall be terminated in the following cases:

1. where the reported breach is manifestly unimportant and does not require further follow-up.

2. of a repetitive report which contains no new information essential to a breach in respect of which an investigation has already been completed, unless new facts or circumstances are presented which warrant further action.

3. When evidence of a crime is established, the report and the accompanying materials are immediately sent to the prosecutor's office.

(2) In the presence of any of the hypotheses described above, the Responsible Officer shall prepare a report to the management of the Company with a proposal to terminate the investigation, and the Company shall determine whether the proceedings should be terminated. Upon termination on the grounds of par. 1, items 1 and 2 above, the Responsible Officer instructs the reporting person that he or she can report to the CPDP as the national authority for external reporting.

## V. REGISTER OF SIGNALS AND SECURITY MEASURES

**Art.21.**(1) Reports shall be documented in the Register of Reports, which shall be kept and maintained on a durable medium by the Responsible Officer. Access to the Register shall be granted only to the Responsible Officer and the

ЗЗЛПСПОИН и служителите на КЗЛД в предвидените в ЗЗЛПСПОИН случаи.

(2) Редът за воденето на регистъра се определя с настоящите правила. Информацията от регистъра се съхранява по начин, позволяващ възпроизвеждането ѝ без загуба на данни и който гарантира нейната поверителност и сигурност. При поддържането, съхраняването, и осъществяването на достъп до Регистъра на сигналите, Служителят по ЗЗЛПСПОИН спазва всички приложими изисквания и вътрешни правила на Дружеството, включително тези, установени в Политиката за защита на личните данни и Политиката за информационна сигурност.

(3) След постъпване на сигнала в регистъра се вписват обстоятелствата, посочени във формуляра.

(4) Служителят по ЗЗЛПСПОИН поддържа актуални данни в регистъра. При допълване на данни в регистъра се прави отбелязване за актуалния статус на сигнала.

(5) Достъпът до информацията, свързана с подадените сигнали, се предоставя единствено на служителите, на които тези данни са необходими за изпълнение на служебните им задължения.

(6) Предаването на данни и ползването на обстоятелства не може да разкрива пряко или косвено самоличността на сигнализиращите лица, както и да създава предположение за тяхната самоличност. В случаите, когато възникне необходимост от включване в проверката на други служители или външни лица, при необходимост, по преценка на Служителя по ЗЗЛПСПОИН, същите подписват декларация за конфиденциалност.

(7) Сигналите и приложените към тях материали, включително последващата документация, свързана с разглеждането им, се съхраняват от Дружеството за срок от 5 години след приключване на разглеждането на сигнала от него, освен при наличието на образувано наказателно, гражданско, трудовоправно и/или административно производство във връзка с подадения сигнал. При закриване или

employees of the CPDP in the cases provided for in the Act.

(2) The procedural rules for keeping the Register are determined by these rules. The information in the Register shall be stored in such a way as to reproduce it without loss of data and to ensure its confidentiality and security. In maintaining, storing, and accessing the Register of Reports, the Responsible Officer shall comply with all applicable requirements and internal rules of the Company, including those set in the Personal Data Protection Policy and Information Security Policy.

(3) After receiving a report, the circumstances indicated in the form shall be entered in the Register.

(4) The Responsible Officer maintains up-to-date data in the Register. The current status of the report is updated each time when data in the Register is supplemented.

(5) Access to the information related to the reports shall be granted only to the employees to whom such data is necessary for the performance of their duties.

(6) The transfer of data and the reliance on circumstances in the Register may not directly or indirectly reveal or suggest the identity of the reporting persons. In cases where there is a need to involve other employees or external persons in the investigation, at the discretion of the Responsible Officer, they shall sign a declaration of confidentiality.

(7) The reports and the accompanying materials, including the subsequent documentation related to their examination, shall be kept by the Company for a period of 5 years after the completion of the investigation of the report, except in the presence of criminal, civil, labor law and/or administrative proceedings in connection with the submitted report. In case of closure or winding down of the Company without legal succession,

заличаване на Дружеството без правоприемник посочената информация и регистъра на сигналите се предават за съхранение в КЗЛД при правила, определени с указания на Комисията.

**Чл.22.** (1) Регистърът за сигнали е електронен и се води и поддържа от Служителя по ЗЗЛПСПОИН на компютър/лаптоп , който е извън мрежата на дружеството. Достъпът до устройството се осъществява чрез парола, която е известна само на служителя/служителите, натоварени с изпълнение на функциите по ЗЗЛПСПОИН и тези Правила. На ръководството на Дружеството се предоставя информация от регистъра, без това да води до разкриване на самоличността на сигнализиращото и засегнатото лице в случаите по чл. 16, т. 11, буква „б“ от ЗЗЛПСПОИН.

(2) На информацията, съдържаща се в определеният за това отделен компютър, веднъж на 3 месеца се създава резервно копие, достъп до което има единствено Служителят по ЗЗЛПСПОИН. Редът, условията и техническите изисквания на Политиката за информационна сигурност, установени в Дружеството са приложими към създаването на резервни копия на регистъра.

(3) Освен регистъра, на изолирания компютър/лаптоп Служителят по ЗЗЛПСПОИН може да съхранява и електронните данни, във връзка с получените сигнали, при спазване на изискванията за сигурност. Електронните документи по сигналите се получават, обработват и съхраняват в електронни папки, с необходимата защита. Документите на хартиен носител по сигналите се съхраняват, организирани в отделни преписки по начин, гарантиращ тяхната поверителност и сигурност.

**Чл.23.** До 31 януари всяка година Дружеството представя на КЗЛД по установения от Комисията ред статистическа информация за предходната година относно броя на

this information and the Register of Reports shall be submitted for storage to the CPDP under rules determined by instructions of the Commission.

**Art.22.**(1) The Register of Reports shall be electronic and shall be kept and maintained by the Responsible Officer on a computer/laptop which is outside the network of the Company. The access to the device is carried out by a password that is known only to the employee(s) entrusted with the performance of the functions under the Act and these Rules. The management of the Company shall be provided with information from the Register, without this leading to disclosure of the identity of the reporting person and the affected person in the cases under Art. 16, item 11, letter "b" of the Act.

(2) The information contained in the designated computer is backed up once every 3 months, with access to the back-up copy available only to the Responsible Officer. The terms, conditions and technical requirements of the Company's Information Security Policy are applicable to the creation of backup copies of the Register.

(3) In addition to the Register, on the designated computer/laptop the Responsible Officer may also store electronic data in connection with the received reports, subject to the applicable security requirements. Electronic documents on reports are received, processed and stored in folders, with the necessary protection. Paper documents on signals shall be stored, organised in separate files in a way that ensures their confidentiality and security.

**Art.23.** By 31 January each year, the Company shall, in accordance with the procedure established by the Commission, submit to the CPDP statistical information for the previous year on the number of



постъпилите сигнали, техният УИН, предмет, броя на извършените проверки и резултатите от тях. За целта служителят по ЗЗЛПСПОИН подготвя доклад с тази информация до ръководството на Дружеството в срок до 15 януари.

## VI. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

**Чл.24.** Настоящите вътрешни правила бяха утвърдени на 03.05.2023 г., като същите следва да се преглеждат най-малко веднъж на три години и да се актуализират при необходимост и промяна на законодателството или вътрешните актове на Дружеството.

**Чл.25.** Правилата се публикуват на интернет страницата на Дружеството и се поставят на общодостъпни и видими места в помещенията на Дружеството, находящи се на гр. Радомир, ул. „Райко Даскалов“ № 68.

Неразделна част от настоящите Вътрешни правила са:

1. Приложение № 1 – Формуляр за регистриране на сигнали по образец, утвърден от Комисията за защита на личните данни;
2. Приложение № 2 - Регистър на подадените сигнали за нарушения по образец, утвърден от Комисията за защита на личните данни.

received signals, their UIN, subject matter, the number of investigations carried out and the results thereof. For this purpose, the Responsible Officer shall prepare a report with this information to the management of the Company by January 15.

## VI. ADDITIONAL PROVISIONS

**Art.24.** These internal rules have been adopted on 03.05.2023 and they should be reviewed at least once every three years and updated if necessary and changed in the legislation or internal acts of the Company.

**Art.25.** The Rules are published on the Company's website and placed in publicly accessible and visible places on the Company's premises, located at 68 Rayko Daskalov str., Radomir.

An integral part of these Internal Rules are:

1. Appendix No 1 – Form for registration of reports in a form approved by the Commission for Personal Data Protection;
2. Appendix No 2 - Register of submitted reports for breaches in a form approved by the Commission for Personal Data Protection.