Whistleblowing Policy

Schwarz Global Services Bulgaria EOOD, UIC 205158327

Version 2.0 of 01.11.2023

General provisions

Art. 1. This Whistleblowing Policy of **Schwarz Global Services Bulgaria EOOD**, Unique Identification Code (UIC) 205158327 (the "**Policy**", respectively the "**Company**"), has been developed in order to **ensure the protection of whistleblowers** or persons publically disclosing information on breaches that has become available to them in the course of or in connection with the performance of their employment duties or in another work-related context relating to the Company's activities, as well as to lay out the procedure for internal reporting.

Art. 2. This Policy has been drawn up in accordance with Bulgarian legislation and, in particular, with the Protection of Persons Reporting or Publicly Disclosing Information on Breaches Act (State Gazette, issue No. 11 of 02.02.2023). The Company encourages all employees to notify the Company and report as soon as possible if they discover breaches.

Art. 3. This Policy **is mandatory for all employees of the Company.** The employees of the company are obliged to render assistance to the officer responsible for handling reports, within the framework of an investigation carried out by such officer under this Policy.

Who handles the submitted reports?

Art. 4. The Company designates its Legal & Compliance Officer (double-hatted Data Protection Officer) as an officer responsible for handling reports. The officer responsible for handling reports shall promptly notify the Company's management (Managers and Procurators) in case of a conflict of interest in the handling of a report, so that another employee can be appointed to receive, register and investigate the report.

The responsible officer shall be functionally independent and shall not receive instructions in relation to the handling of reports. Coordination of the actions of the responsible officer with another employee of the Company is not permitted due to impairment of their functional independence, violation of the obligation of confidentiality and the consequent risk of disclosure of the identity of the reporting person.

How can I report a breach?

Art. 4.1 Reports can be submitted:

a) In writing, signed with a qualified electronic signature, to the email address: sit-bg-compliance@mail.schwarz

b) In writing, signed with a handwritten signature, by mail to the address: 1766 Sofia, "Mladost" district, "Mladost 4" residential district, Business Park Sofia, building 15, 2nd floor, to the attention of the Legal & Compliance Officer.

c) In writing, through the online reporting system available on the following address: https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=2sbg7&c=-1&language=bul - when using this channel, you should familiarize yourself with the information available in the system, including the information regarding the processing of personal data. Please note that the online system is maintained by Schwarz Dienstleistung KG. When submitting a report through the online system, the report will be re-examined by the Company's officer responsible for handling reports.

d) Verbally, on telephone number +359884223404

e) Verbally, through a personal meeting, at a suitable time subject to a prior an appointment with the officer responsible for handling reports in the office of the Legal & Compliance Officer at Sofia, 51 Cherni vrah blvd., floor 11, Office X building.

(2) For the registration of a report, the form contained in Appendix 1 to this Policy, based on a model form approved by the Commission for Personal Data Protection, shall be used. The model form may also be accessed on the website of the Commission on the following address:

https://www.cpdp.bg/?p=sub_rubric&aid=282 (in Bulgarian)

https://www.cpdp.bg/en/index.php?p=sub_rubric&aid=282 (in English)

The report shall contain at least the following information:

a) the sender's three names, address and telephone number, as well as an email address, if any;

b) the names of the person against whom the report is filed and their workplace, if the report is filed against specific persons and they are known;

c) specific details of an actual or potential breach, the place and time of the breach, if already committed, a description of the act or the situation and other circumstances, as far as these are known to the whistleblower;

d) date of submission of the report;

e) signature, electronic signature or other identification of the sender.

(3) If possible, the report must contain details the place, date, time of the breach, persons involved and any other detailed information necessary to investigate the breach. The investigator may request additional information.

(4) **Verbal reports and reports through the BKMS online system are documented by filling in a form under Appendix 1 by the officer responsible for handling reports, who offers the whistleblower to sign it if they wish to do so.**

(5) **If the report does not meet the requirements of this Policy, the whistleblower is sent a message asking them to correct the admitted irregularities within 7 days of**

receiving the report. If the irregularities are not corrected within the said period, the report together with the attachments thereto is returned to the whistleblower.

(6) **Order for reviewing reports:**

The following reports shall be reviewed with priority:

a) reports containing information about committed breaches or a significant risk of committing breaches with a high degree of public danger;

b) reports containing information about committed breaches or a significant risk of committing breaches, requiring immediate action in order to prevent damage or concealment or destruction of evidence.

All other reports are considered in the order of their receipt in the Company.

Art. 5. (1) Every whistleblower shall also be entitled to report externally – by communicating, either orally or in writing, information on breaches to the competent bodies of the Commission for Personal Data Protection. Such external reports may be filed either together with the internal report or independently without any internal report.

(2) The officer responsible for handling reports shall provide the persons willing to submit a report with clear and easily accessible information on the procedures for external reporting to the competent national authority and, where appropriate, to the institutions, bodies, services and agencies of the European Union.

Art. 6. **The Company shall not open proceedings on any anonymous reports or reports relating to breaches committed more than two years earlier.** For these reports no unique identification number shall be generated, no entries shall be made in the register of reported breaches and no statistical information shall be provided to the Commission for Personal Data Protection. Individuals who have anonymously reported breaches not subject to review under this Policy or publicly but anonymously disclosed information on breaches and subsequently been identified and subjected to retaliation are also entitled to protection.

Art. 7. The company shall establish a channel for internal reporting of breaches. The Company and its officer responsible for handling reports shall manage the internal whistleblowing channel in a manner that **ensures the completeness, integrity and confidentiality of information and prevents any unauthorized persons from accessing such information,** and also enables the information saved in a durable medium to be stored for the purposes of investigation of the report and further investigations.

What kinds of breaches can I report?

Art. 8. Any employee or person external to the Company may report actual or potential breaches **in connection with the Company's activities.**

Reports must contain information, including reasonable suspicions, on actual or potential breaches that have been committed or are very likely to be committed within the Company, as well as information on any attempts to conceal breaches, where it concerns breaches of Bulgarian or European legislation.

The areas in which reports of breaches can be filed are as follows:

- public procurement;
- financial services, products and markets and the prevention of money laundering and terrorist financing;
- product safety and compliance;
- transport safety;
- environmental protection;
- radiation protection and nuclear safety;
- food and feed safety, animal health and animal welfare;
- public health;
- consumer protection;
- privacy and personal data protection;
- the security of networks and information systems;
- breaches affecting the financial interests of the EU;
- breaches of internal market rules, including EU rules and Bulgarian legislation on competition and state aid;
- breaches related to cross-border tax schemes;
- committed crime of a general nature, of a person has become aware of in connection with the performance of his/her work or in the course of performance of his/her official duties.
- the rules for payment of due public state and municipal receivables;
- labor legislation;
- the legislation related to the performance of public service.

(**Examples**: theft, threats, violence and criminal damage to property, fraud, money laundering or misappropriation, offering or accepting bribes, financial irregularities, failure to comply with or breach of legal or regulatory requirements, and engaging in or threatening to engage in repressive behavior against a person who has reported or intends to report a breach, etc.)

Who can report?

Art. 9. Reports may be submitted by the following persons:

a) a current or former employee, worker or any other person who is employed by the Company, including a seconded person;

b) a self-employed person;

c) a volunteer or intern;

d) a current or former partner, manager, director, manager, secretary of the Company, member of the audit committee, etc.;

e) a contractor, subcontractors or supplier of the Company (or their employees or subcontractors);

f) a candidate for a job in the Company who has obtained information on a breach in this capacity;

g) any other whistleblower who reports a breach that they become aware of in a work-related context.

(2) Reporting persons shall qualify for protection under this Policy provided that

a) they had reasonable grounds to believe that the information on breaches reported was true at the time of reporting and that such information fell within the scope of Art. 8 hereinabove; and

b) they reported a breach in accordance with this Policy and the law.

If the above requirements are not met, no breach shall be reported under this Policy.

(3) With this Policy, protection is provided to persons reporting through an external channel (to the Commission for Personal Data Protection) or publicly disclosing information on breaches.

Art. 10. This Policy **provides protection to the reporting persons ,** as well as to

a) any persons facilitating whistleblowers in the whistleblowing process;

b) individuals related to the reporting persons (e.g., colleagues or relatives) who may be subject to retaliation on account of reporting;

c) legal entities that the reporting persons own, work for or are otherwise connected with in a work-related context.

Art. 11. (1) It is prohibited to knowingly submit false reports (defamation). Any person who knowingly submits a false report will be subject to disciplinary sanctions, up to and including dismissal. Such events will be reported to the relevant supervisory and law enforcement authorities (e.g. The Commission for Personal Data Protection, the Prosecutor's Office of the Republic of Bulgaria, the Ministry of Interior, as appropriate).

Protection of the whistleblower. Confidentiality.

Art. 12. (1) The Company will not tolerate any type of adverse and injuring retaliatory actions against whistleblowers that are repressive in nature and put the whistleblowers in a disadvantageous position or any threats or attempts at such actions, including but not limited to actions in the form of:

a) temporary suspension, dismissal or application of another ground for termination of the legal relationship under which a person is employed;

b) demotion or delay in promotion;

c) a change in the place or nature of work, the length of working hours or a reduction in remuneration;

d) refusal to provide training to maintain and improve the professional qualification of the worker or employee;

e) negative performance assessment, including in a job recommendation;

f) application of pecuniary and/or disciplinary liability, including imposition of disciplinary sanctions;

g) coercion, rejection, threats to take retaliatory actions or actions, expressed physically, verbally or in any other way, which are intended to harm the dignity of the person and create a hostile professional environment;

h) direct or indirect discrimination, unequal or unfavorable treatment;

i) depriving a worker or employee from the temporary-to-permanent employment contract option, where the worker or employee had a legal right to be offered permanent employment;

j) early termination of a temporary employment contract or refusal to resign such contract, where such option is permissible by law;

k) damages, including to the person's reputation, in particular on social networks, or financial losses, including loss of business and loss of income;

l) inclusion in a list, drawn up on the basis of a formal or informal agreement, in a sector or in an industry, which may result in preventing the person from being employed or from supplying goods or services within such sector or industry (blacklist);

m) early termination or cancellation of a contract for the supply of goods or services when the person is a supplier;

n) termination of a license or permit;

o) directing the person to undergo a medical examination.

(2) An employee who takes action for the purpose of repression against the person filing the report or against a person related to them will be subject to disciplinary sanctions, up to and including dismissal. Such events will be reported to the relevant control and law enforcement authorities (e.g. The Commission for Personal Data Protection, the Prosecutor's Office of the Republic of Bulgaria, the Ministry of Interior, as appropriate).

Art. 13. (1) The company shall treat the information relating to the submitted reports of breaches, the identity of the reporting persons and the persons against whom reports have been filed as confidential. Access to such information shall only be given to the staff members who need the data in order to be able to fulfil their employment duties (need-to-know basis). Typically, a need to know arises for an employee who has a duty to undertake investigative or disciplinary action based on the information.

(2) Disclosure of the identity or information related to a whistleblower's report shall only be permitted with the whistleblower's express written consent, including by email.

(3) Notwithstanding the above paragraphs, the identity of the reporting person and any other information from which the identity of the reporting person may be directly or indirectly deduced may be disclosed only where this is a necessary and proportionate obligation imposed by European Union or Bulgarian legislation in the context of investigations by national authorities or judicial proceedings, including with a view to safeguarding the rights of defence of the person concerned. In such cases the Company

shall notify the reporting persons before their identity or information is disclosed of the need to disclose them. Such notification shall be in writing and shall contain the reasons for the disclosure. The reporting person shall not be informed where information would jeopardise the related investigations or judicial proceedings.

(4) The Company and the officer responsible for handling reports ensure the confidentiality of the information entered in the register of reports. The confidentiality of the information concerning the reporting person and the person concerned shall also be observed at the stage of preparing an individual report on the handling of the report by the officer responsible for handling reports.

Processing of reports

Art. 14. The officer responsible for handling reports shall have the following responsibilities in connection with the processing of received report:

(1) To receive the reports, to generate a unique identification number (UIN) from the system of the Commission on Personal Data Protection (https://www.cpdp.bg/?p=pages&aid=70), and within **7 days after receipt** to confirm their receipt, respectively to notify the whistleblower of any irregularities or that the report is not subject to examination. The notification shall include the UIN and the internal entry number for the report. If the report is verbal, the officer is responsible for documenting it in accordance with Art. 4.1, para. 4. In parallel with the examination of the report, the responsible officer may propose to the managers and procurators of the Company the taking of urgent measures to prevent sabotage of the investigation or which may be necessary to protect the whistleblower.

(2) To ensure that the identity of the whistleblower and any other person named in the report will be properly protected and take the necessary measures to restrict access to the whistleblower by unauthorized persons.

(3) To maintain contact with the whistleblower, requesting additional information from them and third parties if necessary.

(4) To provide feedback to the sender of the report on the actions taken within a period of no longer than **three months** after confirming receipt of the report.

(5) To hear the person against whom the report was filed or accepts their written explanations, then to collect and evaluate the evidence specified by them.

(6) To provide the person concerned with all the collected evidence and give them the opportunity to object to it within 7 days, subject to the protection of the whistleblower.

(7) To provide an opportunity for the person concerned to present and identify new evidence to be collected in the course of the inspection.

(8) In case the facts presented in the report are confirmed:

a) To arrange the taking of follow-up actions in relation to the report, and may require the assistance of other employees of the Company for this purpose.

b) To suggest to the managers and procurators of the Company specific measures to be taken with the aim of stopping or preventing the breach, whether actual or imminent. In these cases, information from the register of reports may be disclosed only to the extent that this does not lead to disclosure of the identity of the reporting person and the person against whom the report was filed.

c) To refer the whistleblower to the competent authorities when his rights are affected.

d) To forward the report to the Commission for Personal Data Protection if it is necessary to take action, and the whistleblower is notified in advance of the referral. In the event that the report is filed against the Company, the officer responsible for handling the report directs the person to simultaneously report to the external whistleblowing authority.

(9) To prioritise the treatment of reports of serious breaches or breaches of essential provisions according to their severity in the event of high inflows of reports.

(10) To close the inspection procedure:

a) in the event that the reported breach is minor and does not require further follow-up actions; closure does not affect other obligations or applicable procedures in relation to the reported breach, or statutory protections with respect to internal or external whistleblowing;

b) regarding repetitive reports which do not contain any meaningful new information adding to a past report in respect of which the relevant procedures were concluded, unless new legal or factual circumstances justify a different form of follow-up;

c) when evidence of a committed crime is found and the report and the materials thereto are sent immediately to the prosecutor's office;

In the cases referred to in a) and b) hereinabove, the whistleblower may submit a report to the Commission for Personal Data Protection.

(11) To draw up an individual report in which it briefly describes the information from the report, the actions taken, the final results of the check on the report, which, together with the reasons, is communicated to the worker or employee who submitted the report and to the person concerned in compliance with the obligation to protect them. In creating the individual report, the confidentiality rules regarding the identity of the reporting person and the person against whom the report was filed remain applicable.

(12) It is permissible for the managers and procurators of the Company to entrust third party natural or legal person with the functions of receiving and registering reports of breaches. It is permissible for such persons to be assigned other, unofficial assistance functions, including conducting an investigation, when this is determined by the nature, seriousness, complexity of the case or the identity of the parties.

Art. 15. Based on the received report and the proposals of the officer responsible for handling the report, the managers and procurators of the Company take action within their competence to stop the breach or to prevent it if it has not started.

Art. 16. (1) The company shall create and maintain a register of reports of breaches, which is not public. The duty to maintain the register rests with the officer in charge of dealing with reports. Access to the register is granted only to the officer responsible for handling reports, as well as the Commission for Personal Data Protection, when requested. Upon receiving a report, the responsible officer should generate a Unique Identification Number (UIN) from the Commission for Personal Data Protection system, which shall be used for the purposes of registering the submitted report. In order to obtain a UIN, the officer responsible for handling the report will have to submit the following information on the website of the Commission for Personal Data Protection:

a) Name and UIC/BULSTAT of the Company;

b) Identification data of the officer responsible for handling the report;

c) Subject of the report (the relevant areas provided for in Art. 8);

d) Method of receipt (written or oral);

(2) The register contains information on:

a) the person receiving the report;

b) the date of submission of the report;

c) the person concerned, if such information is contained in the report;

d) summary data on the alleged breach, such as the place and period of the breach, a description of the act and other circumstances in which it was committed;

e) the connection of the submitted report with other reports, if such connection is identified in the course of the report handling process;

f) information provided as feedback to the person submitting the report and the date it was provided;

g) follow-up actions taken;

h) the results of the report inspection;

i) the report storage period;

j) the internal entry number or similar internal registration number;

k) the UIN.

(3) The information entered in the register is stored in a way that guarantees its confidentiality and security.

(4) The register shall be kept in accordance with the template adopted by the Commission for Personal Data Protection (https://www.cpdp.bg/?p=sub_rubric&aid=283).

(5) In keeping the register, the officer responsible for handling reports shall follow the methodological guidelines of the Commission for Personal Data Protection.

(6) The register shall be kept and maintained on a durable medium - a carrier of information enabling the Company to store information allowing its easy use in the future for a period consistent with the purposes for which the information is intended and which allows the unchanged reproduction of the information stored.

(7) The register is kept in Bulgarian.

(8) Entries into the register as per paragraph 2, item j) and k) above, as well as information that is known from the contents of the report, shall be made immediately. Other information shall be entered gradually, immediately after it becomes known. In the case of a gradual addition of data in the register, the current status of the report shall be noted.

(9) The officer responsible for handling reports is obliged to submit statistical information to the Commission for Personal Data Protection on an annual basis by 31 January. The information shall include the number of received reports, their UIN, subject matter, the number of investigations and their results.

Art. 17. The reports and the materials attached to them, including the subsequent documentation related to their investigation, shall be kept by the Company for a period of 5 years after the completion of the investigation of the report, except in the case of criminal, civil, labor law and/or administrative proceedings in connection with the submitted report, in which case the deadline shall be extended accordingly for the duration of the proceedings. All documentation for the receipt, registration and investigation of reports and their follow-up shall be documented on a durable medium that allows the unchanged reproduction of the stored information as follows:

(1) Paper documents are stored in locked cabinets, access to which is granted only to the officer responsible for handling reports.

(2) Electronic documents, including electronic copies of documents filed on paper, shall be kept in the information system of the Company in a directory, access to which is granted only to the officer responsible for handling reports.

Art. 18. The officer responsible for handling reports forwards to the Commission for Personal Data Protection any report within the scope as per Art. 8 above, for which it was established that:

(1) it informs on violations committed by persons occupying senior public positions under art. 6 of the Anti-Corruption and Forfeiture of Illegally Acquired Assets Act for the purpose of subsequent referral to the Commission for Counteracting Corruption and Forfeiture of Illegally Acquired Assets;

(2) relates to the activities of another obliged entity that is not mentioned in the report (if mentioned in the report, it shall be forwarded to the respective obliged entity instead, if possible);

(3) there is necessity for the Commission to undertake actions required by law.

In the cases above, the responsible officer shall forward the report to the Commission for Personal Data Protection together with all related documentation without deleting any data. The responsible officer shall notify the whistleblower regarding the forwarding of the report.

Art. 19. Together with the management of the Company, the officer responsible for handling reports shall review and update, if necessary, this Policy every three years.

Appendix 1

REPUBLIC OF BULGARIA

COMMISSION FOR PERSONAL DATA PROTECTION

Registration index and date
……../……

(to be completed by the official responsible for the receipt and registration of the report)

REPORT REGISTRATION FORM

FOR THE SUBMISSION OF INFORMATION ON BREACHES UNDER THE WHISTLEBLOWER PROTECTION ACT

IMPORTANT! Please read the instructions on pages 5 and 6 before completing the form.

To be completed by the official receiving the report

UIN	Date

(Unique Identification Number – to be provided by the Central Authority)

METHOD OF SUBMISSION

☐ WRITTEN ☐ VERBAL

IN PERSON ☐ ☐ VIA A PROXY

DETAILS OF THE OFFICIAL RECEIVING, ACCEPTING AND REGISTERING THE REPORT

Name

(forename, middle name and surname)

Position

Workplace

BULSTAT/UIC

To be completed by the person submitting the report if they are using the form as a template for the report

PART I. DETAILS OF THE PERSON SUBMITTING THE REPORT

Name

(forename, middle name and surname)

CONTACT DATA

Region

Location

Mailing Address	
Telephone	e-mail (if available)

☐ I would like to receive a confirmation of the receipt of the report (to be completed only if the report is submitted to the CPDP)

IN THEIR CAPACITY AS	☐ a worker, employee, civil servant or any other person performing wage labour, irrespective of the nature of the work, method of payment and source of funding;
	☐ a person working without an employment relationship and/or in a self-employed capacity and/or engaged in a craft activity
	☐ a volunteer or trainee;
	☐ a partner, shareholder, sole owner of the capital, member of a management or control body of a commercial company, member of the audit committee of an enterprise;
	☐ a person working for a natural person or a legal entity, their subcontractors or suppliers;
	☐ a job applicant who has participated in a competition or any other form of recruitment process and has become aware of a breach in that capacity;
	☐ a worker or employee, when the information was obtained under an employment or official relationship that has been terminated by the time of the report submission or the public disclosure
	☐ another capacity of the person reporting a breach that they became aware of in a work context[1].(please specify)……

PART II. WHOM THE REPORT IS SUBMITTED AGAINST

IDENTIFICATION (in the event of a report against a natural person)	
Name	(forename, middle name and surname)
Workplace	
BULSTAT/UIC	
IDENTIFICATION (in the event of a report against state or municipal authorities or legal entities)	
Name	
BULSTAT/UIC	

PART III. DETAILS OF THE BREACH

1. THE BREACH IS RELATED TO (please mark the field where the breach has occurred)		
☐	a breach of Bulgarian law or of European Union acts in the field of:	
	☐	public procurement;
	☐	financial services, products and markets and the prevention of money laundering and terrorist financing;
	☐	product safety and compliance;
	☐	transport safety;
	☐	environmental protection;
	☐	radiation protection and nuclear safety;
	☐	food and feed safety, animal health and animal welfare;
	☐	public health;
	☐	consumer protection;
	☐	privacy and personal data protection;
	☐	network and information system safety;

[1] Pursuant to §1, item 4 of the Further Provisions of the Whistleblower Protection Act, a "work context" means current and former work activities in the public or private sector through which, irrespective of their nature, persons obtain information about breaches and within which these persons can be subjected to repressive retaliation if they report such information.

☐	a breach affecting the financial interests of the European Union under Article 325 of the Treaty on the Functioning of the European Union;	
☐	a breach of the rules of the internal market under Article 26(2) of the Treaty on the Functioning of the European Union, including the rules of the European Union and of Bulgarian law on competition and state aid;	
☐	a breach related to cross-border tax schemes intended to obtain a tax advantage that contradicts the subject matter or purpose of applicable law in the field of corporate taxation;	
☐	a general offence that the person submitting the report became aware of in conjunction with the performance of their work or official duties.	
☐	breaches of Bulgarian law in the field of:	
	☐	the rules for the payment of public state and municipal receivables due;
	☐	the labour market legislation;
	☐	the legislation related to the performance of civil services.

2. WHEN HAS THE BREACH OCCURRED	
Date/Period	

3. DESCRIPTION OF THE BREACH (specific data on the breach or of the genuine risk of the occurrence of such a breach)

4. LIST OF THE ATTACHED EVIDENCE

PART IV. PERSONS OTHER THAN THE PERSON SUBMITTING THE REPORT WHO NEED PROTECTION

(if known at the time when the report is submitted)

☐	persons assisting the person submitting the report in the course of the process;
☐	persons related to the person submitting the report[2] who could be subjected to retaliation as a result of the report;
☐	legal entities in which the person submitting the report has an equity participation, for which they are working or to which they are related in any other way in a work context.

LISTING/IDENTIFICAITON OF THE PERSONS TO BE GRANTED PROTECTION

CAPACITY OF THE PERSON *(a colleague, a relative – without limitation in degrees, a legal entity in which the person submitting the report has an equity participation, for which*	

[2] Under §1, item 9 of the Further Provisions of the Whistleblower Protection Act, "persons related to the whistleblower (person submitting the report)" means third persons who could be subjected to repressive retaliation in a work context, as colleagues or relatives – without limitation in degree.

they are working or to which they are related in any other way in a work context)	
Name (for natural persons)	(forename, middle name and surname, if known)
Name of the legal entity	BULSTAT/UIC Represented by
CONTACT DATA Location Mailing Address Telephone / E-mail (if any)	

PART V. PERSONS WHO CAN CONFIRM THE REPORTED DATA OR CAN PROVIDE FURTHER INFORMATION

Name (for natural persons)	(forename, middle name and surname, if known)
Name of the legal entity	BULSTAT/UIC Represented by
CONTACT DATA Location Mailing Address Telephone / E-mail (if any)	

THE CURRENT REPORT IS SUBMITTED VIA AN INTERNAL REPORTING CHANNEL:
(to be filled in only when the report is submitted to the CPDP)

☐ YES ☐ NO

INVITATION TO THE PERSON SUBMITTING THE REPORT TO SIGN THE DOCUMENT
(to be marked by the official receiving and registering the report)

☐ ACCEPT ☐ REFUSE

THE REPORT WAS RECEIVED AND REGISTERED BY:

……..……
……

(name of the official)

POSITION:

……

DATE: ..... **SIGNATURE:**

.....

PERSON SUBMITTING THE REPORT/PROXY:

……

…….

(name)

DATE: ..... **SIGNATURE:**

.....

General Information and Completion Instructions:

1. This form is intended for the registration of breach reports via an internal and/or external reporting channel:

• "Internal reporting of information" (to the obliged entities under Article 12 of the Whistleblower Protection Act[3]) means verbal or written communication of information about breaches within a legal entity in the private or public sector;

• "External reporting of information" (before the CPDP) means verbal or written communication of information about breaches to the competent authorities.

2. When completing the form that is to be submitted to the CPDP via the external reporting channel, it has to be indicated whether the report is submitted via an internal reporting channel, as well.

3. IMPORTANT! The form is intended for official use related to the registration of a report by the officials designated by the obliged entities, responsible for the reception and registration of such reports. The form can also be used by the persons submitting reports as a template for a report. In this case the person submitting the report only completes Parts I —V (inclusive).

4. The form is also intended for cases of verbal reporting. In such cases the official designated for the reception and registration of reports documents the report by completing the form. After the completion of the form the official invites the person submitting the report to sign it, if they consent to do so, and marks their consent or refusal in the respective part of the form. The signature must be affixed within 7 days of the invitation.

5. Reports are reviewed when submitted by an individual, in person or via a proxy with an express written power of attorney (no notarisation required), via an external reporting channel or an internal reporting channel, or via public disclosure of information about breaches in a work context.

6. When a report is submitted via a proxy, the original copy of the power of attorney under item 4 must be attached.

---

[3] Obliged entities

Article 12. (*) (1) The obliged entities under this Act shall be the following:

1. employers in the public sector, with the exception of municipalities under Paragraph 2;
2. employers in the private sector with 50 and more workers or employees;
3. employers in the private sector irrespective of the number of their workers or employees if the business activities carried out by them fall within the scope of the legal acts of the European Union specified in Part I-B and Part II of the annex to Article 3(1) and Article 3(3).

(2) Municipalities with a population under 10 000 or less than 50 workers or employees can share resources for the reception of breach reports and follow-up actions on them, provided that they observe the confidentiality obligations.

(3) Obliged entities under Paragraph 1(2) with a total number of workers or employees of 50 to 249 can use a common internal reporting channel, by designating one person or dedicated unit in line with Article 14.

For the official receiving and registering reports:

7. Obtaining a Unique Identification Number is mandatory when registering reports for the purposes of the internal reporting channel. A UIN is generated at CPDP's website. In order to obtain a UIN the official responsible for the reception and registration of reports selects the "Obtain a UIN" option and then enters the following information:

- **Name and UIC/BULSTAT of the employer to whom the report was submitted;**
- **Identification data of the official responsible for the reception and registration of the report;**
- **Subject matter of the report (respective fields of the breach);**
- **Method of submission (written or verbal).**

8. Within the time frame envisaged by law, the person submitting the report is provided with information about the UIN and the registration date of the report.

9. All submitted reports are registered. The circumstances under items 9—11 of these instructions are considered after the completion of the registration and the obtaining of a UIN.

10. No proceedings are launched for anonymous reports and reports related to breaches occurring more than two years ago.

11. Reports are not examined if they do not fall within the scope of the Whistleblower Protection Act or if their content does not provide convincing reasons to perceive them as plausible.

12. Registered reports containing manifestly false or misleading statements and facts are returned with an instruction to the person submitting the report to make corrections to the statements, reminding them of the liability they bear for false accusations under Article 286 of the Criminal Code.

For the person submitting the report:

13. This form can be used by the persons submitting a report as a template. In this case the person submitting the report only completes Parts I —V (inclusive).

14. Within the statutory time limit after the registration of a report, the person submitting the report is provided with information about the registration of the report and its UIN and date. Any subsequent information or communication related to the report is appended under this UIN.

15. Any new information,or information that was not previously stated in the form at the time of its submission can be provided additionally by the person submitting the report. When it is submitted they must specify the UIN obtained for the initial report.

16. Please, keep in mind that:

- **No proceedings are launched for anonymous reports and reports related to breaches occurring more than two years ago.**
- **Registered reports are not examined if they do not fall within the scope of the Whistleblower Protection Act or if their content does not provide convincing reasons to perceive them as plausible.**
- **Registered reports containing manifestly false or misleading statement and facts are returned with an instruction to the person submitting the report to make corrections to the statements, reminding them of the liability they bear for false accusations under Article 286 of the Criminal Code.**

THE SUBMISSION OF REPORTS OR THE PUBLIC DISCLOSURE OF FALSE INFORMATION IS SUBJECT TO ADMINISTRATIVE CRIMINAL LIABILITY UNDER ARTICLE 45 OF THE WHISTLEBLOWER PROTECTION ACT.

Политика за сигнализиране за нарушения

Whistleblowing Policy

Шварц Глобал Сървисис България ЕООД, ЕИК 205158327

Версия 2.0 от 01.11.2023 г.

Общи положения

Art. 20. Настоящата Политика за сигнализиране за нарушения на **„Шварц Глобал Сървисис България“ ЕООД**, ЕИК 205158327 („**Политиката**“, съответно „**Дружеството**“), е разработена с цел да **осигури защитата на лицата, които подават сигнали** или публично оповестяват информация за нарушения, станала им известна при или по повод изпълнение на трудовите им задължения или в друг работен контекст във връзка с дейността на Дружеството, както и да уреди процедурата за вътрешно подаване на сигнали.

Art. 21. Настоящата Политика е изготвена в съответствие с българското законодателство и по-специално със Закона за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения (Обн., ДВ, бр. 11 от 2.02.2023г.). Дружеството насърчава всички служители да уведомяват Дружеството и да докладват възможно най-скоро, ако открият нарушения.

Art. 22. Настоящата Политика **е задължителна за всички служители на Дружеството**. Служителите на дружеството са длъжни да оказват съдействие на служителя, отговарящ за разглеждането на сигнали, в рамките на осъществявано от него разследване по тази Политика.

Кой разглежда подадените сигнали?

Art. 23. Дружеството определя своя Legal & Compliance Officer (съвместяващ функция на длъжностно лице по защита на данните) за служител, отговарящ за разглеждането на сигнали. Служителят, отговарящ за разглеждането на сигнали, своевременно уведомява мениджмънта на Дружеството (Управители и Прокуристи)

в случай на конфликт на интереси при разглеждането на даден сигнал, за да бъде определен друг служител, който да получи, регистрира и разследва сигнала.

Отговорният служител е функционално независим и не получава инструкции във връзка с обработката на сигналите. Не се допуска съгласуване на действията на отговорния служител с друг служител на Дружеството поради накърняване на тяхната функционална независимост, нарушаване на задължението за поверителност и произтичащия от това риск от разкриване на самоличността на лицето, подало сигнала.

Как мога да подам сигнал за нарушение?

Чл.4.1 Сигнали могат да се подават:

f) Писмено, с квалифициран електронен подпис, на имейл адрес: sit-bg-compliance@mail.schwarz

g) Писмено, със саморъчен подпис, по пощата на адрес: гр. София 1766, район „Младост“, квартал „Младост 4“, Бизнес Парк София, сграда 15, ет. 2, на вниманието на Legal & Compliance Officer.

h) Писмено, чрез онлайн система за докладване, достъпна на следния адрес https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=2sbg7&c=-1&language=bul **–** при използването на този канал следва да се запознаете с информацията налична в системата, включително по отношение на обработката на личните данни. Имайте предвид, че онлайн системата се поддържа от Schwarz Dienstleistung KG. При подаване на сигнал през онлайн системата, той отново ще бъде разгледан от служителя в Дружеството, отговарящ за разглеждането на сигнали.

i) Устно, на телефонен номер +359884223404

j) Устно, чрез лична среща, в подходящ срок след уговорка със служителя, отговарящ за разглеждането на сигнали.

(2) За регистрирането на сигнал се използва формулярът по Приложение 1 към тази Политика, по образец утвърден от Комисията за защита на личните данни. Образецът на формуляр е достъпен и на уебсайта на Комисията на следния адрес:

https://www.cpdp.bg/?p=sub_rubric&aid=282 (на български език)

https://www.cpdp.bg/en/index.php?p=sub_rubric&aid=282 (на английски език)

Сигналът следва да съдържа най-малко следната информация:

f) трите имена, адрес и телефон на подателя, както и електронен адрес, ако има такъв;

g) имената на лицето, срещу което се подава сигналът, и неговата месторабота, ако сигналът се подава срещу конкретни лица и те са известни;

h) 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;

i) дата на подаване на сигнала;

j) подпис, електронен подпис или друга идентификация на подателя.

(3) По възможност сигналът трябва да съдържа място, дата, час на нарушението, инволвирани лица и всяка друга подробна информация за разследване на нарушението. Разследващото лице може да поиска допълнителна информация.

(4) **Устни сигнали и сигнали през онлайн системата BKMS се документират чрез попълване на формуляр по Приложение 1 от служителя, отговарящ за разглеждането на сигнали, който предлага на подаващия сигнала да го подпише при желание от негова страна**.

(5) **Ако сигналът не отговаря на изискванията на настоящата Политика, на сигнализиращото лице се изпраща съобщение за отстраняване на допуснатите нередовности в 7-дневен срок от получаване на сигнала. Ако нередовностите не бъдат отстранени в този срок, сигналът заедно с приложенията към него се връща на сигнализиращото лице.**

(6) Ред за разглеждане на постъпилите сигнали:

Следните доклади се разглеждат с приоритет:

а) сигнали, съдържащи информация за извършени нарушения или значителен риск от извършване на нарушения с висока степен на обществена опасност;

б) сигнали, съдържащи информация за извършени нарушения или значителен риск от извършване на нарушения, изискващи незабавни действия с цел предотвратяване на увреждане или укриване или унищожаване на доказателства.

Всички останали сигнали се разглеждат по реда на постъпването им в Дружеството.

Art. 24. (1) Всяко сигнализиращо лице има право и на външно подаване на сигнал - устно или писмено съобщаване на информация за нарушения до компетентните органи на Комисията за защита на личните данни. Такова външно подаване на сигнал може да се подаде заедно с вътрешно подаване или самостоятелно, без вътрешно подаване на сигнал.

(2) Служителят, отговарящ за разглеждането на сигнали предоставя на лицата, желаещи да подадат сигнал, ясна и лесно достъпна информация за процедурите за външно подаване на сигнали към компетентния национален орган, а когато е уместно – към институциите, органите, службите и агенциите на Европейския съюз.

Art. 25. **Дружеството не открива процедура по анонимни сигнали, нито по сигнали, отнасящи се до нарушения, извършени преди повече от две години**. За тези сигнали не се генерира уникален идентификационен номер, не се правят вписвания в регистъра на докладваните нарушения и не се предоставя статистическа информация на Комисията за защита на личните данни. Лицата, които анонимно са подали сигнал не по реда на тази Политика или публично, но анонимно, са оповестили информация за нарушения, като впоследствие са били

идентифицирани и са станали обект на репресивни ответни действия, също имат право на защита.

Art. 26. Дружеството създава канал за вътрешно подаване на сигнали за нарушения. Дружеството и неговия служител, отговарящ за разглеждането на сигнали, управляват канала за вътрешно подаване на сигнали по начин, който **гарантира пълнотата, целостта и поверителността на информацията и възпрепятства достъпа на неоправомощени лица до тази информация**, както и дава възможност за съхранение на записана на траен носител информация за нуждите на проверката по сигнала и за по-нататъшни разследвания.

За какво мога да подавам сигнали за нарушения?

Art. 27. Всеки служител или външно за Дружеството лице може да подава сигнали нарушения или опасност **във връзка с дейностите на Дружеството**.

Сигналите трябва да съдържат информация, включително основателни подозрения, за действителни или потенциални нарушения, които са извършени или е много вероятно да бъдат извършени в Дружеството, както и за опити за прикриване на нарушения, когато това се отнася до нарушения на българското или европейското законодателство.

Областите, в които могат да се подават нарушения са следните:

- обществените поръчки;
- финансовите услуги, продукти и пазари и предотвратяването на изпирането на пари и финансирането на тероризма;
- безопасността и съответствието на продуктите;
- безопасността на транспорта;
- опазването на околната среда;
- радиационната защита и ядрената безопасност;
- безопасността на храните и фуражите, здравето на животните и хуманното отношение към тях;
- общественото здраве;
- защитата на потребителите;
- защитата на неприкосновеността на личния живот и личните данни;
- сигурността на мрежите и информационните системи;
- нарушения, които засягат финансовите интереси на ЕС;
- нарушения на правилата на вътрешния пазар, включително правилата на ЕС и българското законодателство относно конкуренцията и държавните помощи;
- нарушения, свързани с трансгранични данъчни схеми;
- извършено престъпление от общ характер, за което лице е узнало във връзка с извършване на своята работа или при изпълнение на служебните си задължения.

- правилата за заплащане на дължими публични държавни и общински вземания;
- трудовото законодателство;
- законодателството, свързано с изпълнението на държавна служба.

(**Примери**: кражба, заплаха, насилие и престъпни вреди срещу имущество, измами, пране на пари или присвояване на средства, предлагане или приемане на подкуп, финансови нередности, неспазване или нарушаване на законови или регулаторни изисквания и участие или заплаха за участие в репресивно поведение спрямо лице, което е подало сигнал или възнамерява да подаде сигнал за нарушение и мн.др.)

Кой може да подава сигнали?

Art. 28. Сигнал могат да подават следните лица:

h) настоящ или бивш служител, работник или друго лице, което полага наемен труд в Дружеството, включително командировано лице;

i) лице, което упражнява свободна професия;

j) доброволец или стажант;

k) настоящ или бивш съдружник, управител, директор, мениджър, секретар на Дружеството, член на одитен комитет и др.под;

l) изпълнител, подизпълнители или доставчик на Дружеството (или техни служители или подизпълнители);

m) кандидат за работа в Дружеството, получил в това качество информация за нарушение;

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

(2) Лице, подаващо сигнал за нарушения, има право на защита по тази Политика, при условие че

c) 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 8 по-горе; и

d) е подало сигнал за нарушение по предвидения в тази Политика и закона ред.

Ако не са изпълнени горните изисквания, не следва да се подава сигнал за нарушение съгласно тази Политика.

(3) С настоящата Политика се предоставя защита и на лица, подали сигнал през външен канал (към Комисия за защита на личните данни) или които публично са оповестили информация за нарушения.

Art. 29. С настоящата Политика се **предоставя защита на сигнализиращите лица**, както и на

d) лица, които помагат на сигнализиращи лица в процеса на подаване на сигнал;

e) лица, които са свързани със сигнализиращи лица (например, колеги или роднини) и които могат да бъдат подложени на репресивни ответни действия поради сигнализирането;

f) юридически лица, в които сигнализиращото лице притежава дялово участие, за които работи или с които е свързано по друг начин в работен контекст.

Art. 30. (1) Забранено е съзнателното подаване на неверни сигнали (оклеветяване). Лице, което съзнателно подаде неверен сигнал, ще подлежи на дисциплинарни санкции, до и включително уволнение. Такива събития ще бъдат докладвани на съответните контролни и правоприлагащи органи (напр. Комисия за защита на личните данни, Прокуратура на Република България, Министерство на вътрешните работи, според случая).

Защита на Лицето, сигнализиращо за нарушение. Конфиденциалност.

Art. 31. (1) Дружеството няма да толерира какъвто и да е вид ответни неблагоприятни и ощетяващи действия спрямо лица, подаващи сигнали, имащи характера на репресия и поставящи ги в неблагоприятно положение, както и заплахи или опити за такива действия, включително, но не само под формата на:

p) временно отстраняване, уволнение или прилагане на друго основание за прекратяване на правоотношението, по което лице полага наемен труд;

q) понижаване в длъжност или забавяне на повишение в длъжност;

r) изменение на мястото или характера на работата, продължителността на работното време или намаляване на възнаграждението;

s) отказ за осигуряване на обучение за поддържане и повишаване на професионалната квалификация на работника или служителя;

t) отрицателна оценка на работата, включително в препоръка за работа;

u) прилагане на имуществена и/или дисциплинарна отговорност, включително налагане на дисциплинарни наказания;

v) принуда, отхвърляне, заплашване за предприемане на ответни действия или действия, изразени физически, словесно или по друг начин, които имат за цел накърняване на достойнството на лицето и създаване на враждебна професионална среда;

w) пряка или непряка дискриминация, неравностойно или неблагоприятно третиране;

x) 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;

y) предсрочно прекратяване на срочен трудов договор или отказ за повторно сключване, когато такова е допустимо по закон;

z) вреди, включително за репутацията на лицето, по-специално в социалните мрежи, или финансови загуби, включително загуба на бизнес и загуба на доход;

aa) 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 на работа или да не може да достави стока или услуга в този сектор или отрасъл (черен списък);

bb) предсрочно прекратяване или разваляне на договор за доставка на стоки или услуги, когато лицето е доставчик;

cc) прекратяване на лиценз или разрешение;

dd) насочване на лицето към извършване на медицински преглед.

(2) Служител, който предприема действие с цел репресия срещу лицето, подало сигнала, или срещу лице, свързано с него, ще подлежи на дисциплинарни санкции, до и включително уволнение. Такива събития ще бъдат докладвани на съответните контролни и правоприлагащи органи (напр. Комисия за защита на личните данни, Прокуратура на Република България, Министерство на вътрешните работи, според случая).

Art. 32. (1) Дружеството третира като конфиденциална информацията, свързана с подадените сигнали за нарушения и относно самоличността на сигнализиращите лица и лицата, срещу които са подадени сигнали Достъп до такава информация се дава единствено на служителите, на които тези данни са необходими за изпълняване на служебните им задължения (принципът „необходимост да знае“). Обикновено, необходимост да узнае възниква за служител, който има задължение да предприеме действия по разследване или по налагане на дисциплинарна санкция въз основа на информацията.

(2) Разкриването на самоличността на сигнализиращото лице или информацията, свързана с подаден от него сигнал, се допуска само при неговото изрично писмено съгласие, вкл. по мейл.

(3) Независимо от предвиденото в горните алинеи 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 и пропорционално задължение, наложено от българското законодателство или от правото на Европейския съюз в контекста на разследвания от национални органи или на съдебни производства, включително с оглед на гарантиране правото на защита на засегнатото лице. В тези случаите, преди разкриването на самоличността или на информацията, Дружеството уведомява сигнализиращото лице за необходимостта от разкриването им. Уведомлението е писмено и се мотивира. Сигнализиращото лице не се уведомява, когато с това се застрашава разследването или съдебното производство.

(4) Дружеството и длъжностното лице, отговорно за обработването на сигналите, гарантират поверителността на информацията, вписана в регистъра на сигналите. Поверителността на информацията за подателя на сигнала и засегнатото лице се спазва и на етапа на изготвяне на индивидуален доклад за обработването на сигнала от служителя, отговорен за обработването на сигнала.

Обработване на сигнали

Art. 33. Служителят, отговарящ за разглеждането на сигнали има следните задължения по обработване на получен сигнал:

(1) Получава сигналите, да генерира уникален идентификационен номер (УИН) от системата на Комисията за защита на личните данни (https://www.cpdp.bg/?p=pages&aid=70), и в срок от **7 дни след получаването** потвърждава получаването им, съответно уведомява сигнализиращото лице за нередности или че сигналът не подлежи на разглеждане. Уведомлението трябва да включва УИН и вътрешния входящ номер на сигнала. Ако сигналът е устен, отговаря за документирането му по реда на 4.1, ал. 4. Паралелно с разглеждането на сигнала, отговорният служител може да предложи на управителите и прокуристите на Дружеството предприемането на спешни мерки, за да се предотврати саботиране на разследването или които могат да са необходими, за да се предпази сигнализиращото лице.

(2). Гарантира, че самоличността на сигнализиращото лице и на всяко друго лице, посочено в сигнала, ще бъде надлежно защитена и предприема нужните мерки за ограничаване на достъпа до сигнала на неоправомощени лица.

(3). Поддържа връзка със сигнализиращото лице, като при необходимост изисква допълнителни сведения от него и от трети лица.

(4). Предоставя обратна информация на подателя на сигнала за предприетите действия в срок не по-дълъг от **три месеца** след потвърждаването на получаването на сигнала.

(5) Изслушва лицето, срещу което е подаден сигналът или приема писмените му обяснения, след което събира и оценява посочените от него доказателства.

(6) Предоставя на засегнатото лице всички събрани доказателства и му предоставя възможност да направи възражение по тях в 7-дневен срок, при спазване на защитата на сигнализиращото лице.

(7) Предоставя възможност на засегнатото лице да представи и посочи нови доказателства, които да бъдат събрани в хода на проверката.

(8) В случай че изнесените в сигнала факти бъдат потвърдени:

e) Организира предприемането на последващи действия във връзка със сигнала, като за целта може да изисква съдействието на други служители на Дружеството.

f) Предлага на управителите и прокуристите на Дружеството предприемане на конкретни мерки с цел преустановяване или предотвратяване на нарушението в случаите, когато такова е констатирано или има реална опасност за предстоящото му извършване. В тези случаи информация от регистъра на сигналите може да се разкрива, само при условие че това не води до разкриване на самоличността на сигнализиращото лице и на лицето, срещу което е подаден сигналът.

g) Насочва сигнализиращото лице към компетентните органи, когато се засягат неговите права.

h) Препраща сигнала на Комисия за защита на личните данни при необходимост от предприемане на действия, като за препращането сигнализиращото лице се

уведомява предварително. В случай че сигналът е подаден срещу Дружеството, служителят, отговарящ за разглеждането на сигнала, насочва лицето към едновременно сигнализиране на органа за външно подаване на сигнали.

(9) Приоритизира разглеждането на постъпилите множество сигнали за по-тежки нарушения според тежестта на нарушението.

(10) Прекратява проверката:

d) когато нарушението, за което е подаден сигналът, е маловажен случай и не налага предприемането на допълнителни последващи действия; приключването не засяга други задължения или приложими процедури във връзка с нарушението, за което е подаден сигнал, нито законовата защита по отношение на вътрешното или външното подаване на сигнали;

e) 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;

f) когато се установят данни за извършено престъпление, а сигналът и материалите към него се изпращат незабавно на прокуратурата;

В случаите по букви a) и b) сигнализиращото лице може да подаде сигнал до Комисия за защита на личните данни.

(11) Изготвя индивидуален доклад, в който описва накратко информацията от сигнала, предприетите действия, окончателните резултати от проверката по сигнала, които заедно с мотивите съобщава на подалия сигнала работник или служител и на засегнатото лице при спазване на задължението за тяхната защита. При съставянето на индивидуалния сигнал остават приложими правилата за поверителност относно самоличността на подателя на сигнала и лицето, срещу което е подаден сигналът.

(12) Допустимо е управителите и прокуристите на Дружеството да ангажират друго физическо или юридическо лице извън структурата на Дружеството с функциите по приемане и регистриране на сигнали за нарушения. Допустимо е на такива лица да бъдат възложени и други, неофициални функции за съдействие, включително по провеждането на разследване, когато това е обусловено от естеството, сериозността, сложността на казуса или самоличността на страните.

Art. 34. Въз основа на постъпилия сигнал и на предложенията на служителя, отговарящ за разглеждането на сигнала, управителите и прокуристите на Дружеството предприемат действия в рамките на своята компетентност за преустановяване на нарушението или за предотвратяването му, ако то не е започнало.

Art. 35. (1) Дружеството създава и поддържа регистър на сигналите за нарушения, който не е публичен. Задължението за поддържане на регистъра е на служителя, отговарящ за разглеждането на сигнали. Достъп до регистъра имат само длъжностното лице, отговорно за обработването на сигналите, както и Комисията за защита на личните данни при поискване. При получаване на сигнал, отговорният служител следва да генерира Уникален идентификационен номер (УИН) от системата на Комисия за защита на личните данни, който се използва за нуждите на регистриране на подадения сигнал. За получаването на УИН служителят, отговарящ за разглеждането на сигнала, ще трябва да подаде в уебсайта на Комисия за защита на личните данни следната информация:

e) Наименование и ЕИК/БУЛСТАТ на Дружеството;

f) Идентификационни данни на служителя, отговарящ за разглеждането на сигнала;

g) Предмет на сигнала (съответните области, предвидени в Чл. 8);

h) Начин на получаване (писмено или устно);

(2) Регистърът съдържа информация за:

l) лицето, което е приело сигнала;

m) датата на подаване на сигнала;

n) засегнатото лице, ако такава информация се съдържа в сигнала;

o) обобщени данни за твърдяното нарушение, като място и период на извършване на нарушението, описание на деянието и други обстоятелства, при които е било извършено;

p) връзката на подадения сигнал с други сигнали след установяването ѝ в процеса на обработване на сигнала;

q) информация, която е предоставена като обратна връзка на лицето, подало сигнала, и датата на предоставянето ѝ;

r) предприетите последващи действия;

s) резултатите от проверката по сигнала;

t) периода на съхраняване на сигнала;

u) вътрешния входящ номер или друг подобен вътрешен регистрационен номер;

v) УИН

(3) Информацията, вписана в регистъра, се съхранява по начин, който гарантира нейната поверителност и сигурност.

(4) Регистърът се води по образец, приет от Комисията за защита на личните данни (https://www.cpdp.bg/?p=sub_rubric&aid=283).

(5) При воденето на регистъра длъжностното лице, което отговаря за обработването на сигналите, следва методическите указания на Комисията за защита на личните данни.

(6) Регистърът се води и поддържа на траен носител - носител на информация, който позволява на Дружеството да съхранява информация и дава възможност за лесното ѝ използване в бъдеще за срок, съобразен с целите, за които е предназначена информацията, и който позволява възпроизвеждане на съхранената информация в непроменен вид.

(7) Регистърът се води на български език.

(8) Вписванията в регистъра по ал. 2, букви i) и k) по-горе, както и информацията, известна от съдържанието на сигнала, се извършват незабавно. Останалата информация се въвежда постепенно, веднага след като стане известна. При

поетапното добавяне на данни в регистъра се отбелязва текущото състояние на сигнала.

(9) Служителят, отговарящ за разглеждането на сигнали, е длъжен да подава статистическа информация до Комисия за защита на личните данни на ежегоден принцип до 31 януари. Информацията трябва да съдържа броя на получените сигнали, техния УИН, предмета на сигнала, броя на разследванията и резултатите от тях.

Чл. 17. Сигналите и приложените към тях материали, включително последващата документация, свързана с разследването им, се съхраняват от Дружеството за срок от 5 години след приключване на разследването на сигнала, с изключение на случаите на наказателни, граждански , трудовоправни и/или административни производства във връзка с подадения сигнал, като в този случай срокът се удължава съответно за срока на производството. Цялата документация за получаването, регистрирането и разследването на сигналите и тяхното последващо проследяване се документира на траен носител, който позволява възпроизвеждане на съхранената информация в непроменен вид, както следва:

(1) Документите на хартиен носител се съхраняват в заключени шкафове, до които има достъп само длъжностното лице, което отговаря за обработването на сигналите.

(2) Електронните документи, включително електронни копия на документите, подадени на хартиен носител, се съхраняват в информационната система на Дружеството в указател, до който има достъп само длъжностното лице, което отговаря за обработването на сигналите.

Чл. 18. Длъжностното лице, което отговаря за обработването на сигналите, изпраща на Комисията за защита на личните данни всеки сигнал в обхвата по чл. 8 по-горе, за който е установено, че:

(1) съобщава за нарушения, извършени от лица, заемащи висши публични длъжности по чл. 6 от Закона за противодействие на корупцията и за отнемане на незаконно придобитото имущество с цел последващо сезиране на Комисията за противодействие на корупцията и за отнемане на незаконно придобитото имущество;

(2) се отнася до дейността на друго задължено лице, което не е посочено в сигнала (ако е посочено в сигнала, по възможност той се изпраща на съответното задължено лице);

(3) е необходимо Комисията да предприеме действия, които се изискват от закона.

В горните случаи отговорното длъжностно лице препраща сигнала до Комисията за защита на личните данни заедно с цялата свързана документация, без да заличава данни. Отговорното длъжностно лице уведомява подателя на сигнала относно препращането на сигнала.

Чл. 19 Съвместно с ръководството на Дружеството служителят, отговарящ за разглеждането на сигнали, преглежда и актуализира, при необходимост, настоящата Политика на всеки три години.

Приложение 1

Р Е П У Б Л И К А Б Ъ Л Г А Р И Я

КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Регистрационен индекс и дата
……..……/…… г.

(попълва се от служителя, отговарящ за приемането и регистрирането на сигнала)

ФОРМУЛЯР ЗА РЕГИСТРИРАНЕ НА СИГНАЛ

ЗА ПОДАВАНЕ НА ИНФОРМАЦИЯ ЗА НАРУШЕНИЯ СЪГЛАСНО ЗАКОН ЗА ЗАЩИТА НА ЛИЦАТА, ПОДАВАЩИ СИГНАЛИ ИЛИ ПУБЛИЧНО ОПОВЕСТЯВАЩИ ИНФОРМАЦИЯ ЗА НАРУШЕНИЯ

ВАЖНО! Преди попълване на формуляра, моля да се запознаете с указанията на стр. 5 и 6.

Попълва се от служителя, приел сигнала

УИН | **Дата**

(Уникален идентификационен номер – предоставя се от Централния орган)

НАЧИН НА ПОДАВАНЕ

☐ ПИСМЕН ☐ УСТЕН

☐ ЛИЧНО ☐ ЧРЕЗ ПЪЛНОМОЩНИК

ДАННИ ЗА СЛУЖИТЕЛЯ, ПРИЕЛ И РЕГИСТРИРАЛ СИГНАЛА

Име

(собствено, бащино и фамилно)

Длъжност

Месторабота
Наименование

Код по БУЛСТАТ/ЕИК

Попълва се от сигнализиращото лице, в случай че то ползва формуляра като образец за подаване на сигнал

ЧАСТ I. ДАННИ ЗА СИГНАЛИЗИРАЩОТО ЛИЦЕ

Име

(собствено, бащино и фамилно)

ДАННИ ЗА КОНТАКТ

Област

Населено място

Адрес за кореспонденция	

Телефон	Електронна поща (ако има такава)

В КАЧЕСТВОТО МУ НА	☐ работник, служител, държавен служител или друго лице, което полага наемен труд, независимо от характера на работата, от начина на заплащането и от източника на финансирането;
	☐ лице, което полага труд без трудово правоотношение и/или упражнява свободна професия и/или занаятчийска дейност;
	☐ доброволец или стажант;
	☐ съдружник, акционер, едноличен собственик на капитала, член на управителен или контролен орган на търговско дружество, член на одитния комитет на предприятие;
	☐ лице, което работи за физическо или юридическо лице, негови подизпълнители или доставчици;
	☐ кандидат за работа, участвал в конкурс или друга форма на подбор за постъпване на работа и получил в това качество информация за нарушение;
	☐ работник или служител, когато информацията е получена в рамките на трудово или служебно правоотношение, което е прекратено към момента на подаване на сигнала или на публичното оповестяване;
	☐ друго качество на сигнализиращо лице, за нарушение, станало му известно в работен контекст[4].(моля посочете)……

ЧАСТ II. СРЕЩУ КОГО СЕ ПОДАВА СИГНАЛЪТ

ИДЕНТИФИКАЦИЯ (при сигнал срещу физическо лице)	
Име	(собствено, бащино и фамилно, ако е известно)
МЕСТОРАБОТА Наименование	
Код по БУЛСТАТ/ЕИК	
ИДЕНТИФИКАЦИЯ (при сигнал срещу държавни, общински органи или юридически лица)	
Наименование	
Код по БУЛСТАТ/ЕИК	

ЧАСТ III. ДАННИ ЗА НАРУШЕНИЕТО

1. НАРУШЕНИЕТО Е СВЪРЗАНО С (отбележете областта на нарушението)		
☐	нарушение на българското законодателство или на актове на Европейския съюз в областта на:	
	☐	обществените поръчки;
	☐	финансовите услуги, продукти и пазари и предотвратяването на изпирането на пари и финансирането на тероризма;
	☐	безопасността и съответствието на продуктите;
	☐	безопасността на транспорта;
	☐	опазването на околната среда;
	☐	радиационната защита и ядрената безопасност;
	☐	безопасността на храните и фуражите, здравето на животните и хуманното отношение към тях;
	☐	общественото здраве;
		защитата на потребителите;

[4] Съгласно §1, т. 4 от ДР на ЗЗЛПСПОИН - „Работен контекст" са настоящи или минали работни дейности в публичния или в частния сектор, чрез които, независимо от тяхното естество, лицата получават информация за нарушения и в рамките на които тези лица могат да бъдат подложени на репресивни ответни действия, ако подадат такава информация.

	☐	
	☐	защитата на неприкосновеността на личния живот и личните данни;
	☐	сигурността на мрежите и информационните системи;
☐	нарушение, което засяга финансовите интереси на Европейския съюз по смисъла на чл. 325 от Договора за функционирането на Европейския съюз;	
☐	нарушение 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;	
☐	нарушение, свързано 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;	
☐	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.	
☐	нарушения на българското законодателство в областта на:	
	☐	правилата за заплащане на дължими публични държавни и общински вземания;
	☐	трудовото законодателство;
	☐	законодателството, свързано с изпълнението на държавна служба.

2. КОГА Е ИЗВЪРШЕНО НАРУШЕНИЕТО	
Дата/ Период	

3. ОПИСАНИЕ НА НАРУШЕНИЕТО (конкретни данни за нарушението или реалната опасност такова да бъде извършено)

4. ОПИС НА ПРИЛОЖЕНИТЕ ДОКАЗАТЕЛСТВА

ЧАСТ IV. ЛИЦА, РАЗЛИЧНИ ОТ СИГНАЛИЗИРАЩОТО ЛИЦЕ, НА КОИТО ДА СЕ ПРЕДОСТАВИ ЗАЩИТА

(ако са известни към момента на подаване на сигнала)

☐	лица, които помагат на сигнализиращото лице в процеса на подаване на сигнал;
☐	лица, които са свързани със сигнализиращото лице[5] и които могат да бъдат подложени на репресивни ответни действия поради сигнализирането;
☐	юридически лица, в които сигнализиращото лице притежава дялово участие, за които работи или с които е свързано по друг начин в работен контекст.

ИЗБРОЯВАНЕ/ИДЕНТИФИЦИРАНЕ НА ЛИЦАТА, НА КОИТО ДА СЕ ПРЕДОСТАВИ ЗАЩИТА

КАЧЕСТВО НА ЛИЦЕТО	

[5] Съгласно §1, т. 9 от ДР на ЗЗЛПСПОИН -"Лица, свързани със сигнализиращото лице" са трети лица, които могат да бъдат подложени на репресивни ответни действия в работен контекст, като колеги или роднини без ограничение в степените

(колега, роднина без ограничение в степените, юридическо лице, в което сигнализиращото лице притежава дялово участие, за което работи или с които е свързано по друг начин в работен контекст)	
Име (за физически лица)	(собствено, бащино и фамилно, ако е известно)
Наименование (за юридически лица)	Код по Булстат/ ЕИК Представлявано от
ДАННИ ЗА КОНТАКТ Населено място	
Адрес за кореспонденция	
Телефон	Електронен адрес (ако има такъв)

ЧАСТ V. ЛИЦА, КОИТО МОГАТ ДА ПОТВЪРДЯТ СЪОБЩЕНИТЕ ДАННИ ИЛИ ДА ПРЕДОСТАВЯТ ДОПЪЛНИТЕЛНА ИНФОРМАЦИЯ

Име (за физически лица)	(собствено, бащино и фамилно, ако е известно)
Наименование (за юридически лица)	Код по Булстат/ ЕИК Представлявано от
ДАННИ ЗА КОНТАКТ Населено място	
Адрес за кореспонденция	
Телефон	Електронен адрес (ако има такъв)

НАСТОЯЩИЯТ СИГНАЛ Е ПОДАДЕН ПО ВЪТРЕШЕН КАНАЛ:
(попълва се само при подаване на сигнал до КЗЛД)

☐ ДА ☐ НЕ

ПОКАНА ЗА ПОДПИСВАНЕ НА СИГНАЛА ОТ СИГНАЛИЗИРАЩОТО ЛИЦЕ
(отбелязва се от служителя, приел и регистрирал сигнала)

☐ СЪГЛАСИЕ ☐ ОТКАЗ

СИГНАЛЪТ Е ПРИЕТ И РЕГИСТРИРАН ОТ:

……..……

(име на служителя)

ДЛЪЖНОСТ:

……

ДАТА: ..... **ПОДПИС:**

.....

СИГНАЛИЗИРАЩО ЛИЦЕ/ПЪЛНОМОЩНИК:

……

(име)

Вашият сигнал подлежи на проверка за достоверност на основание чл. 15, ал. 6 от ЗЗЛПСПОИН, вкл. по отношение на неговия автор (сигнализиращото лице). Когато има основателни съмнения във връзка със самоличността на сигнализиращото лице (вж. Част I от този формуляр), служителят, отговарящ за разглеждането на сигнала, може да поиска предоставянето на допълнителна информация, необходима за потвърждаване на самоличността му.

Ако се установят неверни или заблуждаващи твърдения за факти и/или след проверката се установи, че лицето, за което се твърди, че е подало този сигнал, не е неговият автор, сигналът и материалите по него ще бъдат препратени на Прокуратурата на Република България по компетентност.

ДАТА: ..... **ПОДПИС:**

.....

Обща информация и указания за попълване:

1. Настоящият формуляр служи за регистриране на сигнали за нарушения чрез канал за вътрешно и/или външно подаване на сигнал.

• „Вътрешно подаване на сигнал“ (пред задължените субекти по чл. 12 от ЗЗЛПСПОИН[6]) е устно или писмено съобщаване на информация за нарушения в рамките на даден правен субект в частния или публичния сектор.

---

[6] Задължени субекти

Чл. 12. (*) (1) Задължени субекти по този закон са:

1. работодателите в публичния сектор с изключение на общините по ал. 2;

2. работодателите в частния сектор с 50 и повече работници или служители;

3. работодателите в частния сектор независимо от броя на работниците или служителите, ако осъществяваната от тях дейност попада в приложното поле на актовете на Европейския съюз, посочени в част I, буква "Б" и част II от приложението към чл. 3, ал. 1 и 3.

(2) Общините с население под 10 000 души или по-малко от 50 работници или служители могат да споделят ресурси за получаване на сигнали за нарушения и за предприемане на последващи действия по тях при спазване на задължението за поверителност.

(3) Задължените субекти по ал. 1, т. 2 с общ брой от 50 до 249 работници или служители могат да използват общ канал за вътрешно подаване на сигнал, като определят едно лице или обособено звено съгласно чл. 14.

• „Външно подаване на сигнал“ (пред КЗЛД) е устно или писмено съобщаване на информация за нарушения на компетентните органи, съгласно ЗЗЛПСПОИН.

2. При попълването на формуляр, подаден до КЗЛД като външен канал, задължително се отбелязва дали сигналът е подаден и по Вътрешен канал.

3. ВАЖНО! Формулярът е предназначен за служебно ползване при регистрирането на сигнал от служителите, определени от задължените субекти, да отговарят за приемането и регистрирането на сигнали. Формулярът може да се ползва и от сигнализиращите лица като образец за подаване на сигнал. В този случай сигнализиращото лице попълва само Част I – V включително.

4. Формулярът е предназначен и за случаите на устно подаване на сигнал. В тези случаи служителят, определен да отговаря за приемането и регистрирането на сигнали, документира сигнала чрез попълване на формуляра. След попълване на формуляра служителят предлага на сигнализиращото лице да го подпише при желание от негова страна и отбелязва неговото съгласие или отказ на съответното място във формуляра, като проверява неговата самоличност чрез представяне на документ за самоличност. Подписът следва да бъде положен в срок не по-късно от 7 дни, след поканата.

5. Разглеждат се сигнали, подадени от физическо лице, лично или чрез пълномощник с изрично писмено пълномощно (не е необходима нотариална заверка), чрез канал за вътрешно подаване на сигнал или канал за външно подаване на сигнал, или публично оповестили информация за нарушения в работен контекст.

6. При подаване на сигнал чрез пълномощник към сигнала се прилага пълномощното по т. 5 в оригинал.

<u>За служителя, приемащ и регистриращ сигнали:</u>

7. Получаването на Уникален идентификационен номер (УИН) е задължително при регистриране на сигнали за нуждите на канала за вътрешно подаване на сигнали. УИН се генерира от сайта на КЗЛД. За получаването на УИН служителят, отговарящ за приемането и регистрирането на сигнали, избира опция „Получаване на УИН“, след което въвежда следната информация:

- **Наименование и ЕИК/БУЛСТАТ на работодателя, при когото е подаден сигналът;**
- **Идентификационни данни на служителя, отговарящ за приемането и регистрирането на сигнала;**
- **Предмет на сигнала (съответните области на нарушение);**
- **Начин на получаване (писмено или устно).**

8. В указания от закона срок на сигнализиращото лице се предоставя информация за УИН и дата на регистриране на сигнала.

9. Регистрират се всички подадени сигнали, попадащи в обхвата на приложното поле на чл. 3 от ЗЗЛПСПОИН. 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 задължения субект.

10. По анонимни сигнали или сигнали, отнасящи се до нарушения, извършени преди повече от две години, не се образува производство.

11. Не се разглеждат сигнали, които не попадат в обхвата на ЗЗЛПСПОИН и съдържанието на които не дава основания да се приемат за правдоподобни.

12. Регистрирани сигнали, съдържащи очевидно неверни или заблуждаващи твърдения за факти, се връщат с указание към сигнализиращото лице за коригиране на твърденията и за отговорността, която носи за набедяване по чл. 286 от Наказателния кодекс.

<u>За сигнализиращото лице:</u>

13. Настоящият формуляр може да се ползва от сигнализиращото лице като образец за подаване на сигнал. В този случай сигнализиращото лице попълва само Част I – V включително.

14. В законоустановения срок след регистриране на сигнал, на сигнализиращото лице се предоставя информация за регистриране на сигнала и неговия УИН и дата. Всяка следваща информация или комуникация във връзка със сигнала се прилага към този УИН.

15. Всяка нова или непосочена при подаването на формуляра информация във връзка със сигнала може да бъде предоставена допълнително от сигнализиращото лице. При подаването ѝ се посочва получения за сигнала УИН.

16. Моля имайте предвид, че:

- **По анонимни сигнали или сигнали, отнасящи се до нарушения, извършени преди повече от две години, не се образува производство.**
- **Не се разглеждат сигнали, които не попадат в обхвата на ЗЗЛПСПОИН и съдържанието на които не дава основания да се приемат за правдоподобни.**
- **Регистрирани сигнали, съдържащи очевидно неверни или заблуждаващи твърдения за факти, се връщат с указание към сигнализиращото лице за коригиране на твърденията и за отговорността, която носи за набедяване по чл. 286 от Наказателния кодекс.**

ЗА ПОДАВАНЕ НА СИГНАЛИ ИЛИ ПУБЛИЧНО ОПОВЕСТЯВАНЕ НА НЕВЯРНА ИНФОРМАЦИЯ СЕ НОСИ АДМИНИСТРАТИВНОНАКАЗАТЕЛНА ОТГОВОРНОСТ ПО ЧЛ. 45 ОТ ЗЗЛПСПОИН.