Multiprint Ltd., 10A Slavyanska Str., 2230 Kostinbrod

APPROVED BY: (**YORDAN BONCHEV**) Date: 12 May 2023

INTERNAL RULES FOR PROTECTION OF INDIVIDUALS REPORTING SIGNALS OR DISCLOSING PUBLICLY INFORMATION ABOUT BREACHES IN "MULTIPRINT" LTD – KOSTINBROD

CHAPTER ONE. GENERAL PROVISIONS

I. Introduction

Article 1. These internal rules, hereinafter referred to as the "Rules," define the conditions and procedure for receiving, reviewing, and taking subsequent actions with regard to signals received by "Multiprint" Ltd. under the Protection of Individuals Reporting Signals or Disclosing Publicly Information about Breaches Act (promulgated in State Gazette No. 11 of 2 February 2023, in force as of 4 May 2023).

II. Definitions

Article 2. For the purposes of these rules, the following definitions apply:

1. "Breaches" are actions or inactions that are: a) not in accordance with Bulgarian legislation and are related to areas referred to in Article 3, or b) contrary to the subject or purpose of the rules in acts of the European Union and the areas referred to in Article 3.
2. "Employer" is any natural person, legal entity, or its division, as well as any other organizational and economic entity (enterprise, institution, organization, cooperation, enterprise, establishment, household, partnership, and similar) that independently hires workers or employees under labor and employment relationships, including remote work and work for performance of work in the enterprise - user.
3. "Information about a breach" is information, including reasonable suspicions, about actual or potential breaches that have been committed or are very likely to be committed in the organization where the reporting person works or has worked, or in another organization with which they have been or were in contact during their work, as well as attempts to conceal breaches.
4. "Work context" refers to present or past work activities in the public or private sector through which, regardless of their nature, individuals obtain information about breaches and within which these individuals may be subjected to repressive retaliatory actions if they provide such information.
5. "Affected individual" is a person or legal entity indicated when submitting the signal or disclosing information as a person to whom the breach is attributed or with whom this person is associated.
6. "Feedback" is the provision of information to the reporting person about the action that is planned or has already been taken as a subsequent action, as well as the reasons for this subsequent action.

7. "Isolation" is an action or inaction aimed at isolating the individual who has reported the signal or publicly disclosed information about a breach from the professional environment.
8. "Enterprise" is any natural person, legal entity, or civil partnership engaged in economic activity, regardless of ownership, legal and organizational form.
9. "Persons associated with the reporting person" are third parties who may be subjected to repressive retaliatory actions in the work context, such as colleagues or relatives without limitation in degrees.
10. "Repeatedly" refers to the breach committed within a one-year period from the entry into force of the penal order imposing a penalty for the same type of breach.
11. "Retaliatory actions" are any direct or indirect action or inaction occurring in a work context caused by internal or external signal reporting or public disclosure, which causes or may cause unfavorable consequences damaging the reporting person.
12. "Subsequent actions" are any actions taken by the recipient of the signal or by a competent authority to assess the accuracy of the statements presented in the signal and, where appropriate, to treat the reported breach, including actions such as internal investigation, inquiry, criminal prosecution, measures to secure evidence, or concluding the procedure.
13. "Sufficient data" are data from which a reasonable assumption can be made about a breach falling within the scope of this law.
14. "Obviously minor breach" is present when the committed breach reveals a clearly insignificant degree of public danger due to the absence or insignificance of harmful consequences.
15. "Serious breach" is present when the committed breach has or could have a significant and lasting negative impact on the public interest.
16. "Internal signal reporting" is oral or written communication of information about breaches within a legal entity in the private or public sector.
17. "External signal reporting" is oral or written communication of information about breaches to competent authorities.
18. "Durable carrier" is any carrier of information that allows obligated entities under Article 12, paragraph 1, or the Commission to store information, which allows its easy future use for a period corresponding to the purposes for which the information is intended and which allows unchanged reproduction of the stored information.
19. "Privacy protection" is any intervention in personal space within the meaning of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

III. Protected Individuals (Signal Reporting or Public Disclosure)

Article 3. (1) The Protection of Individuals Reporting Signals or Disclosing Publicly Information about Breaches Act aims to provide protection to individuals who report signals or publicly disclose information about breaches of Bulgarian legislation or acts of the European Union, which has become known to them in connection with the performance of their labor or official duties or in another work context. (2) Protection is provided to the reporting person from the moment of submitting the signal or publicly disclosing information

about a breach. (3) A reporting person within the meaning of the Protection of Individuals Reporting Signals or Disclosing Publicly Information about Breaches Act is a natural person who submits a signal or publicly discloses information about a breach known to them as:

1. an employee, worker, or other individual engaged in hired labor, regardless of the nature of the work, the method of payment, and the source of funding;
2. an individual engaged in work without an employment relationship and/or practicing a liberal profession and/or a craft;
3. a volunteer or intern;
4. an individual working for a person or legal entity, its subcontractors, or suppliers;
5. a job applicant participating in a competition or another form of selection for employment and who has received information about a breach in this capacity;
6. an employee or worker when the information has been obtained within a labor or official relationship that has terminated by the time of submitting the signal or public disclosure. (4) Protection under the Protection of Individuals Reporting Signals or Disclosing Publicly Information about Breaches Act is also provided to any other reporting person who submits a signal about a breach known to them in a work context. (5) Protection under this law is also provided to:
    1. individuals assisting the reporting person in the process of submitting a signal;
    2. individuals associated with the reporting person who may be subjected to repressive retaliatory actions due to the reporting;

IV. Conditions for the Protection of Reporting Individuals

Article 4. (1) An individual submitting a signal about breaches through an internal or external channel within the meaning of the Protection of Individuals Reporting Signals or Disclosing Publicly Information about Breaches Act has the right to protection, provided that:

1. there was reasonable cause to believe that the information about the breach in the signal was true at the time of its submission and that this information falls within the scope of Article 3 of the Protection of Individuals Reporting Signals or Disclosing Publicly Information about Breaches Act;
2. the signal about the breach was submitted under the conditions and procedure of the Protection of Individuals Reporting Signals or Disclosing Publicly Information about Breaches

Act. (2) If the conditions under paragraph 1 are met, the right to protection is also extended to the individual who submits a signal about a breach to institutions, authorities, services, or agencies of the European Union. Such submission of a signal is considered submission through an external channel.

V. Conditions for the Protection of Individuals Publicly Disclosing Information about Breaches

Article 5. An individual who publicly discloses information about a breach has the right to protection when there was reasonable cause to believe that the information about the breach was true at the time of its disclosure and that this information falls within the scope of Article 3 of the Protection of Individuals Reporting Signals or Disclosing Publicly Information about Breaches Act, and one of the following conditions has been met:

1. the individual has submitted a signal under the conditions and procedure of this law, but no corresponding actions have been taken on the signal within the deadlines provided in Sections I and II of Chapter Two;
2. the individual has reasonable grounds to believe that:

   a) the breach may pose an immediate or obvious threat to the public interest, or there is a risk of damage that cannot be remedied;

   b) in the case of external signal reporting, there is a risk of retaliatory actions or there is a likelihood that the breach will not be effectively reviewed due to a risk of concealment or destruction of evidence, suspicion of a secret agreement between the competent authority and the violator, or involvement of the authority in the breach, as well as other specific circumstances specific to the case.

VI. Barriers to Initiating Proceedings

Article 6. (1) Proceedings are not initiated for:

1. anonymous reports;
2. reports relating to breaches committed more than two years ago.

(2) The rights granted to individuals under the Protection of Individuals Reporting Signals or Disclosing Publicly Information about Breaches Act cannot be restricted. Any provision in a public law act or clause in a private law act that excludes or limits their rights is void.

VII. Right to Protection for Anonymously Submitted Signal

Article 7. Individuals who have anonymously submitted a report, not in accordance with this law or who have publicly, but anonymously, disclosed information about breaches, and have subsequently been identified and subjected to repressive retaliatory actions, have the right for protection when the conditions under Article 4, paragraph 1, and Article 5 of these rules are met.

CHAPTER TWO. REPORTING SIGNALS

I. Requirements for Establishing an Internal Reporting Channel

Article 8. (1) Pursuant to Article 12, Paragraph 1 of the Protection of Persons Reporting Signals or Disclosing Information about Breaches Act, "Multiprint" Ltd., as an obligated entity under this law, has established an internal reporting channel for breaches, which meets the following requirements:

1. It is managed in a manner that ensures the completeness, integrity, and confidentiality of the information and prevents unauthorized access to this information.
2. It provides the possibility of storing recorded information on a durable medium for the needs of the signal's verification and for further investigations.
3. It is communication-secured, operates through a phone, email address, a mailbox for submitting signals, access to which is only available to the employee responsible for reviewing signals.

(2) "Multiprint" Ltd. provides clear and easily accessible information regarding the conditions and procedure for submitting signals. The information is provided on the company's website (www.multiprint.bg) and is visibly displayed in the printing house building ("Annex 1 -

Notice to Natural Persons under the Protection of Persons Reporting Signals or Disclosing Information about Breaches Act").

II. Employees Responsible for Reviewing Signals

Article 9. (1) In "Multiprint" Ltd., with an order from the director, an employee responsible for reviewing signals is designated - Georgi Ivanov, who performs his duties in compliance with the Protection of Persons Reporting Signals or Disclosing Information about Breaches Act.

(2) The employee responsible for reviewing signals should not have a conflict of interest for each reviewed case. In case of a conflict of interest, the employee issues a written abstention, and the signal is reviewed by another designated employee according to the director's order.

III. Submitting a Signal

Article 10. (1) The signal is submitted to the employee responsible for reviewing signals in writing, including via email, or orally. Oral submission of a signal can be done over the phone, through other voice messaging systems, or upon the signaling person's request - through a personal meeting within an agreed appropriate period.

(2) A template form is used for registering signals in "Multiprint" Ltd. (Annex No. 3 - "Signal Submission Form"), containing the following data:

1. The full name, address, and phone number of the submitter, as well as an email address if available.
2. The names of the person against whom the signal is submitted and their workplace, if the signal is against specific individuals and they are known.
3. Specific information about the breach or the real danger of its occurrence, the place and period of the breach, if committed, a description of the action or circumstance, and other known circumstances of the signaling person.
4. Date of signal submission.
5. Signature, electronic signature, or other identification of the submitter.

(3) The written signal is submitted by the submitter by filling out the form in Paragraph 2. The oral signal is documented by the employee responsible for reviewing signals by offering the signaling person to sign it if desired.

(4) Any kind of information sources supporting the claims made in it and/or references to documents, including data about individuals who could confirm the reported information or provide additional information, can be attached to the signal.

(5) If the signal does not meet the requirements in Paragraph 1, the signaling person is sent a message to rectify the detected irregularities within a 7-day period from receiving the signal. If the irregularities are not rectified within this period, the signal, along with its attachments, is returned to the signaling person.

(6) Each signal is checked for its credibility. Signals that do not fall within the scope of the Protection of Persons Reporting Signals or Disclosing Information about Breaches Act and whose content does not provide grounds for being considered plausible are not reviewed. Signals containing obviously untrue or misleading statements of facts are returned with instructions to the submitter to correct the statements and the responsibility they bear for misleading.

(7) In case the signal is received by an unauthorized person, the same is obliged to hand it over to the employee responsible for reviewing signals within 24 hours or on the next business day, maintaining confidentiality regarding its content.

(8) The internal reporting channel for breaches is accessible at: - Email address: givanov@multiprint.bg (by submitting the "Signal Submission Form" - Annex No. 3); - Address: Kostinbrod, 10A "Slavyanska" Str., "Multiprint" Ltd. - for Mr. Georgi Ivanov (by submitting the "Signal Submission Form" - Annex No. 3); - Phone number: 0888 721 771;

IV. Working with Signals. Internal Investigation

Article 11. The employee responsible for reviewing signals must:

1. Receive signals and acknowledge their receipt within 7 days of receiving them.
2. Ensure that the identity of the signaling person and any other individuals mentioned in the signal will be properly protected and take necessary measures to limit unauthorized access to the signal.
3. Maintain communication with the signaling person, requesting additional information from them and third parties when necessary.
4. Provide feedback to the signal submitter on the actions taken within a period not exceeding three months from confirming the signal's receipt.
5. Provide individuals wishing to submit a signal with clear and easily accessible information about the procedures for externally submitting signals to the competent national authority and, when appropriate, to the institutions, authorities, services, and agencies of the European Union.
6. Document oral signals.
7. Maintain a registry of submitted signals.
8. Listen to the person against whom the signal is submitted, accept their written explanations, and collect and assess the evidence they provide.
9. Provide the affected person with all gathered evidence and give them the opportunity to object to it within a 7-day period, while respecting the protection of the signaling person.
10. Allow the affected person to present and provide new evidence that may be collected during the investigation.
11. If the facts presented in the signal are confirmed: a) Organize further actions related to the signal, which may involve the cooperation of other individuals or departments within the structure of "Multiprint" Ltd. b) Suggest to the employer to take specific measures to cease or prevent the breach in cases where it has been identified or there is a real danger of its occurrence. c) Direct the signaling person to the competent authorities when their rights are affected. d) Refer the signal to the external reporting authority if necessary actions are required from them, with prior notification to the signaling person; in the event that the signal is submitted against the signaling person's employer, the employee responsible for reviewing the signal directs the individual to simultaneously report to the external reporting authority.
12. Provide information to the Commission for Personal Data Protection about the received signal and receive a unique identification number from the CPDP.

13. Regularly provide the necessary statistical information to the CPDP according to its established procedure, including, if technically feasible, by establishing a direct connection between the registry of the obligated entity and the registry maintained by the national authority for external signal submission.

V. Subsequent Actions

Article 12. (1) The employer:

1. Based on the received signal and the suggestions of the employee responsible for reviewing the signal according to Article 16, item 11, letter "b," takes actions within its competence to cease the breach or prevent it if it has not yet occurred.
2. Prioritizes the review of received signals for more severe breaches according to predetermined criteria and rules.
3. Terminates the investigation: a) When the breach reported in the signal is minor and does not require additional follow-up actions; the conclusion does not affect other obligations or applicable procedures related to the breach for which the signal was submitted or the protection under this law regarding internal or external signal submission. b) For a repeated signal that does not contain new materially relevant information about a breach for which an investigation has already been concluded unless new legal or factual circumstances provide grounds for subsequent actions. c) When data about a committed crime is established; the signal and related materials are promptly sent to the prosecutor's office.
4. Prepares an individual report briefly describing the information from the signal, the actions taken, the final results of the signal investigation, which, along with the reasons, is communicated to the signaling person and the affected individual, while respecting their protection.

(2) In cases where the investigation is terminated based on Article 1, item 3, letters "a" and "b," the signaling person may submit a signal to the national authority for external signal submission.

VI. Registry of Signals

Article 13. (1) "Multiprint" Ltd. establishes and maintains a registry of signals for breaches, which is not public (Annex No. 2 - "Registry of Signals").

(2) The registry contains information about:

1. The person who received the signal.
2. The date of signal submission.
3. The affected individual, if such information is present in the signal.
4. Summarized data about the alleged breach, including the place and period of the breach, a description of the action, and other circumstances under which it was committed.
5. The connection of the submitted signal to other signals identified during and throughout the processing of the signal.
6. Information provided as feedback to the signal submitter, including the date of provision.

7. Subsequent actions taken.
8. The results of the signal investigation.
9. The period of signal retention.

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

(4) The procedure for maintaining the registry is determined by a decision of the employer in accordance with the regulation of the national authority for external signal submission.

(5) The employee responsible for reviewing signals must regularly provide the necessary statistical information to the national authority for external signal submission according to its established procedure, including, if technically feasible, by establishing a direct connection between the registry of the obligated entity and the registry maintained by the national authority for external signal submission.

CHAPTER THREE. ADDITIONAL RULES APPLICABLE TO SIGNAL SUBMISSION

I. Confidentiality Obligation

Article 14. (1) "Multiprint" Ltd. has implemented appropriate measures to protect information related to submitted signals for breaches and to protect the identity of the signaling individuals, ensuring access to this information only by the employee who requires it for the performance of their official duties.

(2) The transmission of data and referencing circumstances must not directly or indirectly reveal the identity of the signaling individual or create assumptions about their identity.

(3) Paragraphs 1 and 2 also apply to protecting the identity of affected individuals.

(4) Disclosure of identity or information as per Paragraph 1 is permitted only with the explicit written consent of the signaling individual.

(5) Regardless of Paragraph 1, the identity of the signaling individual and any other information that can directly or indirectly reveal their identity may only be disclosed when necessary and proportionate obligations imposed by Bulgarian legislation or European Union law in the context of investigations by national authorities or judicial proceedings, including to ensure the right to defense of the affected individual.

(6) In cases under Paragraph 5, before disclosing identity or information under Paragraph 1, "Multiprint" Ltd. informs the signaling individual of the necessity for such disclosure. The notification is in writing and is reasoned. The signaling individual is not notified if it endangers the investigation or judicial proceedings.

(7) The employee who receives information about a breach, including trade secrets, is obligated not to use or disclose trade secrets for purposes beyond those necessary for subsequent actions.

II. Processing of Personal Data

Article 15. (1) Any processing of personal data carried out under these rules, including the exchange or transmission of personal data by competent authorities, is conducted in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680, and when

involving institutions, authorities, services, or agencies of the European Union, in accordance with Regulation (EU) 2018/1725, as well as the Personal Data Protection Act.

(2) Personal data that are evidently irrelevant to the consideration of a specific signal are not collected, and if accidentally collected, they are erased.

CHAPTER FOUR. MEASURES FOR ENSURING PROTECTION

I. Prohibition of Retaliatory Actions Against Individuals Who Have Submitted a Signal or Publicly Disclosed Information about Breaches

Article 16. (1) Any form of retaliatory action against individuals mentioned in Article 3, which has the character of repression and puts them in an unfavorable position, as well as threats or attempts of such actions, including in the form of:

1. temporary suspension, dismissal, or application of another basis for terminating the employment relationship of an employee;
2. demotion or delay of promotion;
3. change of workplace or job nature, duration of working time, or reduction of remuneration;
4. denial of training for maintaining and improving the professional qualification of a worker or employee;
5. negative evaluation of work, including in recommendations for work;
6. imposition of pecuniary and/or disciplinary liability, including disciplinary penalties;
7. coercion, rejection, threats to take retaliatory actions or actions expressed physically, verbally, or in any other way with the intention of damaging the dignity of the person and creating a hostile professional environment;
8. direct or indirect discrimination, unequal or unfavorable treatment;
9. deprivation of the opportunity to transition from a fixed-term employment contract to an indefinite-term employment contract when the worker or employee had a legal right to be offered permanent employment;
10. premature termination of a fixed-term employment contract or refusal to renew when permissible by law;
11. damages, including to the person's reputation, especially on social media, or financial losses, including loss of business and loss of income;
12. inclusion in a list based on an official or unofficial agreement that may result in the person being unable to work or provide goods or services (blacklist);
13. premature termination or disruption of a contract for the supply of goods or services when the person is a supplier;
14. termination of a license or permit;
15. directing the person to undergo a medical examination.

(2) The competent authorities under Article 20, paragraph 1 of the Protection of Whistleblowers Act shall issue mandatory instructions to cease harmful actions under paragraph 1 until the conclusion of the investigation conducted by them.

II. Liability for Damages

Article 17. In the event of a breach of the prohibition under Article 33, the signaling individual has the right to compensation for both material and non-material damages suffered.

III. Support Measures

Article 18. (1) Individuals under Article 3 have the right to access the following support measures:

1. free and accessible information and advice on the procedures and protective measures under Articles 36, 37, 38, and 39 of the Protection of Whistleblowers Act;
2. assistance from any authority necessary for their protection against retaliatory actions, including proper notification that they have the right to protection under this law;
3. legal assistance in criminal, civil, administrative, and international disputes related to civil cases, concerning the protection of the signaling individual in connection with the submitted signal or disclosed information, in accordance with the Legal Aid Act;
4. extrajudicial resolution of cross-border disputes through mediation in accordance with the Mediation Act.

(2) The measures under paragraph 1, items 1 and 2 are provided by the Commission for Personal Data Protection, the measures under item 3 are provided by the National Legal Aid Bureau, and the measures under item 4 are provided by a mediator registered in the Unified Register of Mediators.

IV. Exemption from Liability

Article 19. (1) Signaling individuals are not held liable for acquiring the information for which the signal is submitted or which is publicly disclosed, or for accessing it, provided that this acquisition or access does not constitute a separate offense.

(2) Signaling individuals are not held liable for violating restrictions on disclosing information provided by a contract, legal or sub-legal act, or administrative act, provided that they have reasonable grounds to believe that submitting the signal or publicly disclosing the information was necessary to reveal the breach.

(3) When an individual submits a signal or publicly discloses information about breaches, and this information includes trade secrets and when that individual meets the conditions of the Protection of Whistleblowers Act, such submission of the signal or public disclosure is considered lawful within the meaning of Article 7, paragraph 2 of the Trade Secret Protection Act.

V. Damages Caused to Private Legal Entities

Article 20. Damages caused to the signaling individual in connection with the signal submitted by them or publicly disclosed information are considered to be intentionally caused until proven otherwise.

VI. Protection of Affected Individuals

Article 21. (1) The affected individual has the right to full defense and a fair trial, as well as the presumption of innocence, including the right to be heard and the right to access relevant documents.

(2) The affected individual has the right to compensation for all material and non-material damages when it is established that the individual under Article 3 knowingly submitted a signal with false information or publicly disclosed false information, and when the circumstances would have required them to assume that the information is false.

VII. Liability for Actions or Inactions Not Related to Submitting the Signal

Article 22. (1) The signaling individual is liable under Bulgarian law and Union law for actions or inactions not related to submitting the signal or not necessary to disclose the breach.

(2) In a judicial or administrative legal process where an individual claims to have been subject to retaliatory actions under Article 33 of the Protection of Whistleblowers Act, it must be proven that these actions are a reaction specifically to the signal submitted by them. It should not be assumed that the retaliatory action was taken in response to the signal submitted by the individual if the assessment of all circumstances indicates that the imposing party had another lawful basis for applying the measure.

FINAL PROVISIONS

§ 1. "Multiprint" Ltd. conducts a review of its internal signaling rules and subsequent actions at least once every three years, analyzes the practice of implementing this law, and updates the rules when necessary.

§ 2. These rules are approved by Order of the Manager of "Multiprint" Ltd. dated May 4, 2023.

§ 3. These rules will be updated after the publication of the Regulation for the Implementation of the Law on the Protection of Individuals Submitting Signals or Publicly Disclosing Information about Breaches and the Appendices published therein.

Appendices:

- Appendix No. 1 "Notification to Persons under the Law on the Protection of Individuals Submitting Signals or Publicly Disclosing Information about Breaches";
- Appendix No. 2 "Register of Signals";
- Appendix No. 3 "Signal Submission Form".