POLICY FOR INTERNAL REPORTING OF INFORMATION ON BREACHES

1. GENERAL PROVISIONS

1.1 Scope of the Policy

This Policy describes the internal channel for reporting of Information on Breaches at IBM Bulgaria EOOD (the "**Company**", "**we**", "**us**") and the subsequent actions in relation to their processing and has been developed on the grounds of Art. 13, para. 2 of the *Protection of Persons Who Report or Publicly Disclose Information on Breaches Act*[1] *("**Protection of the Reporting Persons Act**")*.

This Policy is an IBM document specific to Bulgaria and concerns the employees and contractors of IBM Bulgaria EOOD. This document regulates the procedure for Bulgaria for reporting Breaches at or concerning the Company which fall within the scope of the EU Whistleblowing Directive[2] and the Protection of the Reporting Persons Act. This Policy supplements the "**IBM Group Policy**" which regulates the terms and conditions for submitting concerns via the Employee Concerns Program, and which applies for all IBM companies within the IBM group, part of which is IBM Bulgaria EOOD. In the event of a discrepancy between the IBM Group Policy and this Policy, the procedures set out in this Policy shall apply where the reported Breaches fall within the scope of the Bulgarian Protection of the Reporting Persons Act and are within the areas listed in section 3 below. This does not necessarily mean that the employees of the Company are restricted from using all available means for reporting a Breach as offered by IBM, as they choose to do. In such cases, any Report which falls under the scope of this Policy shall be transferred to the Contact Persons to be reviewed under this Policy.

The possibility of reporting Breaches is open not only to our employees but for all persons who have received Information about Breaches at or concerning the Company, during or in connection with the performance of their employment or work duties or in any other work context. The procedure described below applies to all Reports related to Breaches within the scope of the Protection of the Reporting Persons Act.

1.2 Purpose of the Policy

It is essential for a functioning compliance system to recognise and address Breaches at an early stage so they can be remedied without delay and the current system can be adapted, if necessary. This requires that all employees are vigilant and willing to report if they consider that they have Information on actual or potential Breach within the scope of section 3 of this Policy. The Company has therefore implemented an internal reporting channel that provides confidential means of communication to report possible Breaches and ensure that the Reports are clarified in a transparent, efficient, and objective manner.

The internal reporting channel is introduced with the expectation that it will be used responsibly by all Reporting Persons and that it will only be used to report Breaches within the scope of this Policy.

1.3 Definitions

Whenever used in this Policy, the following terms shall have the following meaning:

Breach/es means a breach(es) of the applicable Bulgarian or European legislation in connection with or arising from the Company's activities which are illegal or unacceptable because they are contrary to the object or purpose of the rules in the acts of the EU (see section 3 below).

Information on/about a Breach/es is information, including reasonable suspicion, about actual or potential Breaches that have occurred or are likely to occur at the Company or otherwise affecting the Company.

Report/s is/are report(s) of Information about (potential) Breaches to the Contact Persons.

---

[1] Promulgated, SG No. 11/2.02.2023, effective 4.05.2023.

[2] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, OJ L 305, dated 26.11.2019, p.17 -56.

Contact Person/s is/are the local person(s) responsible for handling Reports, including receiving and processing the submitted Reports, communicating with the Reporting Person and informing the Reporting Person about the actions taken in relation to the submitted Report. The Company's Contact Persons are set out in section 5 below.

Reporting Person/s is/are all person(s) who have obtained Information about Breaches during or in connection with the performance of their employment or work duties or in any other work context.

Person/s Concerned is/are the natural or legal person(s) identified in the Report as the person(s) to whom the Breach is attributed or with which that Breach is associated.

Retaliation is any direct or indirect act or omission which occurs in a work context, which is a reaction to a Report, and which causes or is likely to cause detriment to the Reporting Person.

Final Report is the final act under Art. 17, para. 1, sub-para. 4 of the Protection of the Reporting Persons Act that the Contact Persons prepare on behalf of the Company after the completion of the verification of a specific Report.

2. PROTECTING OF THE REPORTING PERSONS

Regardless of whether the Reports are made under this Policy or under the procedures set in the IBM Group Policy, the persons who report Breaches honestly and in good faith are entitled to protection which includes **(i) keeping the Reporting Person's identity confidential and (ii) protection from acts of Retaliation**.

Confidentiality shall also be kept in terms of the identity of the Person(s) Concerned or other persons named in the Report.

With respect to Reports made under this Policy, the obligation to maintain confidentiality will not apply if state or local government authorities or competent courts demand the disclosure of certain information in compliance with the law. The Reporting Person will be informed in advance of the disclosure of their identity, unless the respective authority or court has informed the Company that notifying the person would jeopardise the relevant investigation, verification, or legal proceedings.

Reporting persons who report Breaches under this Policy, will be **exempt from liability for obtaining, accessing, and disclosing the information**, unless obtaining or accessing the reported information constitutes a criminal offence. Reporting Persons will also not be held responsible for disclosure, provided that they have reasonable grounds to consider that the information is true and that the reporting is necessary to reveal the Breach.

3. BREACHES, WHICH REQUIRE REPORTS

Actual or potential Breaches of applicable laws of the Republic of Bulgaria and/or the EU, in the areas listed below, **in or affecting the Company**, are to be reported through the internal reporting channel.

In particular, individuals should report under this Policy where they have Information about the following Breaches in or affecting the Company:

(a) Breaches of applicable legislation in the area of public procurement;

(b) Breaches of applicable legislation in the area financial services, prevention of money laundering and financing terrorism;

(c) Breaches of product safety regulations or other product-related regulations;

(d) Breaches of transport safety regulations;

(e) Breaches of applicable legislation in the area of protection of the environment;

(f) Breaches of radiation protection and nuclear safety regulations;

(g) Breaches of food and feed safety, animal health and welfare regulations;

(h) Breaches of public health regulations;

(i) Breaches of applicable legislation in the area of consumer protection;

(j) Breaches of privacy, personal data protection regulations, and network and information systems security;

(k) Breaches affecting the financial interests of the European Union, and breaches of internal market rules, including rules on European Union and Bulgarian legislation on competition and State aid;

(l) Breaches of corporate tax rules or arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law;

(m) General offences of which the person became aware in a work context;

(n) Violation of the rules for payment of outstanding public state and municipal entitlements;

(o) Labour law violations and violations related to the performance of government service.

4. METHODS OF REPORTING

In the event of a violation of Bulgarian or EU law, in or affecting the Company, Reporting Persons can submit Reports in one or more of the following ways:

(i) via the internal reporting channel of the Company, or

(ii) to the Commission for Personal Data Protection (CPDP), which acts as national external reporting office, at: city of Sofia 1592. 2, Prof. Tsvetan Lazarov Blvd., e-mail: whistleblowing@cpdp.bg, website: www.cpdp.bg, or

(iii) by public disclosure of the Information about the Breach, subject to the conditions for doing so in the Protection of the Reporting Persons Act.

Reporting Persons may choose to report in one way, a combination of two ways, or all three ways at the same time.

The Company encourages all employees and Reporting Persons to prioritise Reports **via the internal reporting channel** to ensure prompt and effective handling of Reports and prompt follow up by the Company.

5. IMPORTANT INFORMATION ON THE SUBMISSION OF A REPORT THROUGH THE INTERNAL CHANNEL

All Reporting Persons, whether they are part of the Company's structure or have received Information about a Breach in another work context, can submit written or verbal Reports by sending them to the Contact Persons and in the manner as specified in this section 5 of the Policy.

Reports must be submitted to any or all of the following local Contact Persons at the Company:

- **Daniela Velichkova**, CFO, IBM Bulgaria and EET
- **Boyka Docheva**, Technology Lifecycle Services, Global Delivery and CEE HRP

Reports can be submitted to the Contact Persons **verbally** or **in writing**.

Reporting Person can submit a written Report by completing the standard form, approved by CPDP (the "**Report Form**"), and sending it to the Contact Persons:

(a) by email to any or all of the following email addresses:

- daniela.velichkova@ibm.com
- boyka.docheva@bg.ibm.com

(b) by postal mail to the Company's address, as follows: *1766 Sofia, Mladost Region, Residential District Mladost IV, Business Park Sofia, Building 5B*, with a note on the envelope stating that the item is for the attention of the above Contact Persons or to any of them.

Reporting Persons, who are not currently employed in the Company, can download the Report Form from IBM Bulgaria website.

The Company's current employees can download the Report Form from https://w3.ibm.com/w3publisher/human-resources-at-ibm-bulgaria/whistleblowing-policy. The Company encourages all employees to complete the Report Form and submit their Reports in English language.

The Company's current employees may also submit written Reports via the Employee Concerns Program by completing the submission form, available on the following link: https://w3.ibm.com/hr/employee-concerns/#/home/employee-concerns. Reports for Breaches that fall within the scope of this Policy and are submitted via the Employee Concerns Program shall be transferred to the local Contact Persons to be reviewed under this Policy if the Reporting Person has provided his/her names and contact details. Anonymous Reports which are submitted via the Employee Concerns Program shall not be reviewed under this Policy.

Reporting Person can submit a verbal Report by arranging a personal meeting with the Contact Persons. Personal meetings shall be arranged in advance by calling any of the following telephone numbers:

- for personal meeting with Daniela Velichkova: +359-884-616435
- for personal meeting with Boyka Docheva: + 359-888-99-03-22

Employees who have reason to believe that a conflict of interest would arise in the handling of a particular Report by both of the Contact Persons, may submit their Report to the Employee Concerns administrator at appeals@us.ibm.com or by phone at (914)499-4147 (USA). In this case, the Employee Concerns administrator shall register the Report in accordance with this Policy.

6. PROCESSING REPORTS

6.1 Responsibility for Processing of Reports

The Company's Contact Persons are responsible for receiving and handling Reports.

Contact Persons also performs other duties in accordance with their positions in the Company's structure. On a case-by-case basis, upon receipt of a Report, the Contact Persons shall ensure that the reconciliation of their other duties does not result in a conflict of interest. In the event of a suspected conflict of interest after receiving the Report, depending on the circumstances, the Report will be reviewed in accordance with this Policy by the other Contact Person or by another person - part of the Company's structure.

Depending on the nature of the Report and the area in which it falls, persons from the IBM group structure (the "**Investigators**") may be involved in the verification of the information on the Report, subject to the requirements for ensuring the security and confidentiality of the information and the identity of the Reporting Person.

6.2 Submitting Reports

Persons who have Information about a Breach should submit a Report by one of the methods set forth in section 4 of this Policy, preferably through the Company's internal reporting channel.

Written Reports can be submitted at any time by sending the completed Report Form, using the methods of reporting set out in Section 5 above.

Verbal Reports can be submitted during the established working hours of the Company. Where the Report is submitted verbally, the Contact Persons shall document the Report by completing the Report Form with the information received from the Reporting Person, providing the Reporting Person an opportunity to review the completed information, make any comments or corrections, and sign the completed Report Form if they choose.

Non-anonymous written Reports that are submitted via Employee Concerns Program and fall within the scope of this Policy, shall be documented by the Contact Persons in the same manner as the verbal Reports.

Anonymous Reports will not be reviewed under this Policy.

Reports relating to Breaches committed more than two years ago shall not be considered. If the Contact Persons receive such Report, the Report, together with its annexes, shall be returned to the Reporting Person. Where the Reporting Person is currently employed in the Company, the Contact Persons can advise him/her to submit their Report via the Employee Concerns Program.

Reports must always be complete, truthful, objective and unbiased, and contain sufficient specific information to allow verification.

In particular, the Report must contain specific details of the Breach or of a real risk of it being committed, the place and time of the Breach, a description of the act or the circumstances and such other circumstances that are known to the Reporting Person.

The Reporting Person may attach to the Report any type of information supporting the allegations made in the Report and/or documents, including reference to persons who could confirm the reported data or provide additional information.

All non-anonymous Reports that are submitted through the internal channel and fall within the scope of section 3 of this Policy, receive a Unique Identification Number (UIN), which the Contact Persons generate from CPDP's website.

Reporting Persons will receive confirmation of receipt of the non-anonymous Report from the Contact Persons within **seven days** of receipt at the latest. The confirmation shall include information of the UIN which was generated from CPDP's website.

Where the Report is for Breach which does not fall within the scope of section 3 of this Policy, the Contact Persons shall send a notice to the Reporting Person in which they return the Report and its attachments, stating the reason why the Report will not be considered. Where the Reporting Person is currently employed in the Company, the Contact Persons can advise him/her to submit their Report via the Employee Concerns Program. If the nature of the Report requires consideration by another competent authority, the Contact Persons may refer the Reporting Person to that authority.

6.3 Formal Verification of Reports

After receiving the Report, the Contact Persons shall check:

(a) whether the Report contains all the necessary data - the Contact Persons shall check whether the Report contains the required data in accordance with the approved Report Form. Where irregularities are found, the Contact Persons shall, send a notice to the Reporting Person to rectify them within seven days of receipt of the notice. If the irregularities are not rectified within the time limit specified, the Report, together with its annexes, shall be returned to the Reporting Person. Where the Reporting Person is currently employed in the Company, the Contact Persons can advise him/her to submit their Report via the Employee Concerns Program.

(b) whether the Report is plausible - the Contact Persons assesses whether the facts described in the Report are plausible in purely factual terms. Where the content of the Report does not support a finding that it is plausible, the Contact Persons shall send a notice to the Reporting Person to rectify their statements within seven days of receipt of the notice. If the statements are not rectified within the time limit specified and the described facts still cannot be considered plausible, the Report, together with its annexes, shall be returned to the Reporting Person stating the reason why the Report will not be considered. Where the Reporting Person is currently employed in the Company, the Contact Persons can advise him/her to submit their Report via the Employee Concerns Program.

Where the Report contains clearly false or misleading statements, the Contact Persons shall send a notice to the Reporting Person to clarify their statements within seven days of receipt of the notice and inform them of the responsibility for allegations. If the statements are not clarified within the time limit specified, the Report, together with its annexes, shall be returned to the Reporting Person. .

When a Report is returned in the above-mentioned cases, the Contact Persons shall return an e-mail, if such was provided by the Reporting Person, or issues a protocol, indicating the date of receipt of the Report and the date and ground for its return.

6.4 Investigating the Facts

If the Report is plausible and there is no ground to return it to the Reporting Person, the Contact Persons and the Investigators proceed with an investigation of the facts stated in the Report.

The aim of the investigation is to determine whether or not the (possible) Breaches addressed by a Report exist.

For this purpose, the Contact Persons and the Investigators are entitled to contact the Reporting Person and the other persons, named in the Report, and - if necessary - conduct interviews with them and request and inspect necessary documents.

Investigations are conducted in an objective and impartial manner under the presumption of innocence.

The Person Concerned will be informed that they are the subject of an investigation and of their rights as a Person Concerned, and of their rights under data protection legislation applicable in the Republic of Bulgaria and under this Policy.

In the course of the investigation, the Contact Persons and the Investigators:

(a) will hear the Person Concerned and/or accept their written explanations;

(b) will collect and evaluate the evidence referred to by the Person Concerned;

(c) will provide the Person Concerned with all the evidence collected and will give them the opportunity to object to it within **seven days**, while preserving the confidentiality of the identity and ensuring the protection of the Reporting Person;

(d) will give the Person Concerned the opportunity to submit and identify new evidence to be collected in the course of the investigation.

The Contact Persons and the Investigators shall take into account all findings and collected evidence when assessing the facts of the case and deciding on follow-up measures.

The Contact Persons and the Investigators can obtain support in the investigation from other persons who are part of the Company's structure or who are employees of another company – part of IBM group, as well as obtain external support (e.g. by lawyers, auditors, other experts) provided that the confidentiality requirements are observed and if it seems appropriate and necessary to adequately clarify the facts.

No later than **three months** of the acknowledgement of receipt of the Report, the Contact Persons shall provide feedback to the Reporting Person on the action taken in relation to the Report received. The information shall be provided irrespective of whether the investigation has been completed or is still ongoing.

6.5 Completion of the investigation

The Contact Persons and the Investigators will complete the investigation when:

(a) there is sufficient confirmation of the facts to be able to reliably assess that the (possible) Breach addressed by a Report does not exist/was not committed, or

(b) there is sufficient confirmation of the facts to be able to reliably assess that the (possible) Breach addressed by a Report exists, or

(c) further clarification of the facts by reasonable means seems impossible or unjustified.

Upon completion of the investigation, the Contact Persons shall prepare a proposal setting out the results of the completed investigation and propose to the Company:

(a) to terminate the procedure for processing the Report in cases where:

(i) it is established that the Breach referred to in the Report does not exist;

(ii) further clarification of the facts by reasonable means seems impossible or unjustified;

(iii) the reported Breach is minor and does not require follow-up action;

(iv) the Report is about a Breach for which an investigation has already been conducted and completed and the resubmitted Report does not contain new information relevant to the Breach alleged in the Report;

(v) evidence of a criminal offence is established, in which case the Report and its accompanying material shall be sent immediately to the public prosecutor's office.

(b) to take specific follow-up measures to stop or prevent the Breach in cases where it has been detected or there is a real risk of such being committed.

If the facts stated in the Report are confirmed, the Contact Persons also:

(a) arrange for follow-up action to be taken in relation to the Report, and for that purpose may require the assistance of other persons or units within the structure of the Company. This right of the Contact Persons may be exercised in combination with the proposal to the Company to take specific measures and insofar as the functions performed by the Contact Persons allow it.

(b) refer the Reporting Person to the competent authorities where their rights are affected;

(c) forward the Report to the Commission for Personal Data Protection when:

(i) the alleged Breach is committed by person(s) holding senior public position under Art. 6 of the Counter-Corruption and Unlawfully Acquired Assets Forfeiture Act, or

(ii) the Report relates to the activity of another obliged entity without it being specifically mentioned in the Report, or

(iii) the Commission for Personal Data Protection is required to take actions under the Protection of the Reporting Persons Act.

The Contact Persons shall forward the Report and all documentation and collected evidence thereto to the Commission for Personal Data Protection no later than 7-days after the circumstances set out in p. (i) to (iii) have been established. In any case of forwarding of a Report, the Reporting Person shall be informed in advance of the forwarding.

6.6 Final Report

Upon completion of the investigation and receipt of a proposal from the Contact Persons, the Company, through its Contact Persons, prepares a Final Report outlining the information from the Report, the actions taken and the results of the investigation and the follow-up action immediately taken or to be taken, including specific follow-up actions taken by the Company to stop or prevent the Breach.

The Company, through the Contact Persons, informs the Reporting Person and the Person Concerned of the result of the investigation, by observing their rights hereunder. The Final Report will not be provided to these persons.

6.7 Analysis and Follow-up Measures

After the investigation has been completed, the Contact Persons will check whether the Report or the information obtained in the course of the investigation has revealed deficits or weaknesses in the Company’s procedures and processes and propose appropriate measures to the Company’s management.

The Company, through its designees, shall implement the specific follow-up actions and measures identified in the Final Report to stop or prevent the Breach, and shall incorporate the information received with a view to improve the Company's procedures and processes.

6.8 Data Protection

If personal data are processed in the course of processing the Reports, this will be done in compliance with the provisions of the Personal Data Protection Act[3] and the General Data Protection Regulation ("**GDPR**")[4].

The legal basis for processing personal data when handling Reports are:

- Where reporting Breaches of the law is concerned, the Company is obliged to process this data in accordance with Art. 6 (1) c) of the GDPR in conjunction with the Protection of the Reporting Persons Act.
- Where processing other Reports is concerned, the legal basis is Art. 6 (1) f) of the GDPR; the Company has a legitimate interest in maintaining its reputation and ensuring compliance with its rules and policies.

Personal data that are clearly not relevant to the consideration of the specific Report shall not be collected and, if accidentally collected, shall be deleted.

7. RECORD OF THE REPORTS

The Company shall establish and approve a template Register of the Reports of Information on Breaches (the "**Register**").

7.1 Procedure for Keeping and Maintenance of the Register

The Register is kept and maintained by the Contact Persons. The Register is maintained in Bulgarian language.

The Register is not public. The Register shall be created, maintained, and stored in electronic form with controlled access. Only the Contact Persons shall have access to the Register through individual username and password. Access to the information in the Register may exceptionally be granted to other persons who, in accordance with the Protection of the Reporting Persons Act and the regulations adopted thereunder, are expressly authorised with the right of access.

7.2 Obligations of the Contact Persons with regard to the Register

The Contact Persons are required to register in the Register all non-anonymous Reports that are received through the internal reporting channel and fall within the scope of section 3 of this Policy.

When completing the information in the Register, the Contact Persons are obliged to correctly enter all data from the received Report, to monitor for inconsistencies and missing data in the Report and to take the necessary actions for their timely removal and clarification. The Contact Persons are responsible for marking the current status of registered Report depending on the processing stage of the Report as follows:

a. status "not to be considered" refers to Reports for breaches committed more than 2 years ago;

b. status "in the process of rectifying irregularities" refers to Reports for which the Contact Persons have sent notice for rectification of irregularities because:

   (i) the Report which does not contain the information required by law, and/or

   (ii) the Report contains statements which do not provide a basis for considering the report plausible, and/or

[3] Promulgated, SG No. 1/4.01.2002, effective 1.01.2002, last amended and supplemented, SG No. 11/2.02.2023, effective 4.05.2023

[4] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Promulgated, Official Journal of the EU 04.05.2016, L 119, p. 1- 88, effective from 25.05.2018

(iii) the Report contains clearly false or misleading statements;

c. status “returned” relates to Reports for which the Reporting Persons have not rectified the irregularities within the time limit provided;

d. status “under investigation” relates to Reports which are not returned and investigation procedures have started;

e. status “closed” refers to Reports for which a Final Report has been issued;

f. status “forwarded to competent authorities” refers to Reports which were forwarded to the Commission for Personal Data Protection or to the public prosecutor's office.

The Contact Persons shall take and comply with all technical and organisational measures specified in point 8 to ensure the confidentiality and security of the information in the Register.

The Contact Persons are obliged to submit to the Commission for Personal Data Protection by 31 January with the statistical information for the preceding year on the number of Reports received through the internal reporting channel, their UIC, their subject matter, the number of inspections carried out and their results..

8. STORING OF REPORTS. TECHNICAL AND ORGANISATIONAL MEASURE TO ENSURE THE CONFIDENTIALITY AND SECURITY OF THE INFORMATION FROM THE REPORTS REVEIVED

The Reports, as well as any and all documents and information in relation thereto, as well as the information on any and all actions taken by the contacts person, or by the Company, and the information in the Register shall be stored on a durable medium (paper and/or an electronic carrier) for a period of 5 (five) years from the date of completion of the actions under the Report, unless otherwise specified by law or sub-legislative norms.

8.1 Hard copy Reports and Documents

Reports, documents and information, received on hard copy, including verbal Reports, when registered by the Contact Persons by filling in a card copy Report Form, shall be stored in the Company’s premises.

The Company shall take the following technical and organisational measures to ensure the confidentiality and security of the submitted hard copy Reports, documents and information:

8.1.1 Reports and documents shall be stored in special locked cabinets accessible only by the Contact Persons.

8.1.2 Reports and documents shall not be moved outside the Company's premises except when it is necessary to forward them to a competent authority or return them to the Reporting Person.

8.1.3 The Contact Persons may create electronic copies of submitted hard copy Reports and documents, which shall be stored in accordance with Section 8.2 below.

8.1.4 The Company's premises where the hard copy Reports and documents are stored are subject to 24/7 physical and/or technical security (through signalling and security technology and video surveillance) and implemented procedures for control of the physical access.

8.2 Electronic Reports and Documents

Reports that are submitted electronically, including verbal Reports, when registered by the Contact Persons by filling in an electronic Report Form, and the documents in relation thereto, are stored on a server in shared folders with restricted access.

The Company shall take the following technical and organizational measures to ensure the confidentiality and security of electronically submitted Reports and the documents in relation thereto:

8.2.1 Only the Contact Persons have direct access to the folders in which the electronic Reports and the documents in relation thereto are stored, through individual usernames and passwords (known to each of them only, respectively).

8.2.2 Where necessary the Contact Persons can grant limited and restricted by time access to a specific case file to third persons, by strictly observing the rules therefore under this Policy.

8.2.3 Electronic Reports and documents shall be protected by maintaining security and anti-virus programs to ensure that the completeness, integrity and confidentiality of the information is maintained and that unauthorized persons are prevented from accessing such information.

8.2.4 Copies and backups are created to restore information.

8.2.5 Unauthorised access shall be controlled by systems that store history logs of the operations with the documents.

9. FINAL PROVISIONS

At least once every three years, the Company shall revise this Policy, taking into account the analyses of the effectiveness of the procedures made by the Contact Persons.

IBM BULGARIA EOOD