REPORTING OF BREACHES HANDBOOK

of

IBM ROMANIA S.R.L.

This Handbook is issued on the basis of Law no. 361/2022 on the protection of public interest whistleblowers, published in the Official Gazette of Romania, Part I, no. 1218 of 19 December 2022 (the "**Whistleblower Protection Law**").

With this Handbook we would like to introduce you to the terms and conditions under which you can submit information on breaches, including reasonable suspicion, about actual or potential breaches, **at or affecting IBM Romania S.R.L.** (the **"Company"**).

1. WHO CAN REPORT?

You can and should report if, in the course of your employment or official duties or in any other professional-related context, you become aware of information about a breach at or affecting the Company. Our reporting channel is open not only to our employees, but to all persons who have information about breaches at or affecting the Company.

2. WHAT KIND OF BREACHES CAN YOU REPORT?

You can report if you believe that you have information about breaches of Romanian and European legislation in connection with or arising from the activities of the Company in the areas provided by Article 3 para. 1 of the Whistleblower Protection Law.

Attention! You should not be concerned if you do not have sufficient knowledge to identify the breach, but you have reliable information or a reasonable suspicion that it may have been committed or is very likely to be committed. Please notify the Company as set out below in any such case.

Specifically, you may report if you have information or suspicions about the following breaches, at or affecting the Company:

- ✓ Breaches of applicable legislation in the area of public procurement;
- ✓ Breaches of applicable legislation in the area financial services, prevention of money laundering and financing terrorism;
- ✓ Breaches of product safety regulations or other product-related regulations;
- ✓ Breaches of transport safety regulations;
- ✓ Breaches of applicable legislation in the area of protection of the environment;
- ✓ Breaches of radiation protection and nuclear safety regulations;
- ✓ Breaches of food and feed safety, animal health and welfare regulations;
- ✓ Breaches of public health regulations;
- ✓ Breaches of applicable legislation in the area of consumer protection;
- ✓ Breaches of privacy, personal data protection regulations, and network and information systems security;

- ✓ Breaches affecting the financial interests of the European Union, and breaches of internal market rules, including rules of European Union and Romanian legislation on competition and State aid;
- ✓ 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.

3. HOW CAN YOU REPORT?

You can report one or more of the following ways:

- ✓ through the Company's internal reporting channel; or
- ✓ to the National Integrity Agency (*in Romanian*: 'Agentia Nationala de Integritate'), at: Bucharest, 15 Lascăr Catargiu Bld., 010661, District 1, e-mail: avertizari@integritate.eu, telephone +40 372 069 869, website: avertizori.integritate.eu; or
- ✓ by publicly disclosing information about the breach, subject to the conditions laid down in the Whistleblower Protection Law.

You can choose the reporting method as one, a combination of two ways, or all three ways at the same time, with the observance of the legal provisions regarding public disclosure. **We encourage you to prioritise reports via the internal reporting channel of the Company** so that they can be handled promptly and efficiently.

4. HOW CAN YOU USE THE INTERNAL CHANNEL OF THE COMPANY?

You may report a breach by submitting your report to any of the following employees who have been appointed by Company to be responsible for the handling of reports (**"Contact persons"):**

- **Fanel Enache**, CFO, Director, IBM Romania, telephone +40 726 166 488;
- **Cerasela Baiculescu**, Country Leader IBM Romania and Moldova, Director, telephone +40 731 790 480;
- **Alexandra Buzoianu**, HR Leader – IBM Consulting CICs CEE, telephone +40 731 035 195.

in one of the following ways:

- ➢ **by email**, to the following email address: whistleblowingromania@ibm.com;
- ➢ **by post,** to the address of the Company in Bucharest, as follows: **Bucharest, 15D Șoseaua Orhideelor, The Bridge, Building A, 5th floor, 060071, District 6**, marked 'CONFIDENTIAL', with a note on the envelope stating that the item is for the attention of one or all of the above-mentioned Contact Persons;
- ➢ **verbally**, by **telephone** or through a **personal/ on-line meeting** arranged with one of the Contact Persons.

Verbal reports can be submitted during Company business hours. Meetings shall be arranged in advance by calling any of the telephone numbers of the Contact Persons listed above.

Written reports (by email or by post) can be submitted at any time.

Reports should contain (i) the name and contact details of the reporting person, (ii) details regarding the professional context in which the information was obtained, (iii) the Person(s) concerned, if known to the reporting person, (iv) the description of the alleged Breach and (iv) the date and signature of the reporting person (for written reports only)

Reports may also be submitted **anonymously**, in which case the elements at points (i) and (iv) above are not mandatory. **Please note that by submitting an anonymous report without providing any valid contact details, you understand and agree that the Contact Person(s) will not be able to reach you, including for the purpose of requesting additional information. It is your responsibility to ensure that any such report contains all information required for the analysis and resolution of the alleged Breach(es).**

If you are a current employee at IBM Romania S.R.L., you can also submit a written report online through the "Employee Concerns" Program, which is available only for Company's employees. When submitting a report through "Employee Concerns", please provide your contact details so that we can get in touch with you, if necessary, to clarify the information in the report and to inform you of the progress and action taken on the report you submitted.

Your report must be as **complete, truthful, objective, and unbiased as possible** and contain **sufficient specific information** to allow verification. 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 as **far as they are known**. You may attach to your report any documents or information to support your allegations, and you may also refer to persons who could confirm the data reported by you or provide additional information.

Anonymous reports may also be submitted by Company's employees through "Employee Concerns". However, such reports shall not be transferred to the local Contact Persons and/or processed under this Policy.

We encourage you to report a breach **as soon as** you become aware of it or have established it so that we can act on it as promptly and effectively as possible.

5. WHAT HAPPENS AFTER YOU REPORT A BREACH?

When you report a breach through the Company's internal channel and valid contact details were provided, the Contact Persons will notify you within 7 days after receipt of the report that the report has been received.

The Contact Persons will verify reports that are truthful and justified. Reports that contain clearly false or misleading statements shall be returned to you, where possible, with instructions to rectify the statements. The report will be dismissed without further examination and returned to you, where possible, if it does not contain the necessary information for verification and you have not rectified the irregularities within 15 days as of the notice provided by the Company. The same resolution will be applied to anonymous reports that do not contain sufficient information for the analysis and resolution of the alleged breach(es).

The Contact Persons will get in touch with you if you have to provide further information in connection with the report.

No later than 3 months after the acknowledgement of receipt of the report, the Contact Persons will provide feedback to you on the actions taken in relation to your report. The information will be provided irrespective of whether the verification has been completed or is still ongoing. You shall be kept informed whenever

developments are recorded, except for the case where such information would jeopardize the investigation and/or implementation of follow-up measures.

Upon completion of the verification, you will be informed of the final result of this verification.

6. WHAT PROTECTION DO YOU HAVE IF YOU REPORT A BREACH?

When you report a breach and you had grounds to believe that the information on the breach in the report was correct at the time of its submission, **you are guaranteed the following protections:**

- Confidentiality

Your identity will be kept confidential and will not be disclosed to others, either during or after the completion of the verification of the report, unless required by the law or with your written consent.

- Protection from retaliation

You and any third-party person connected with you will be protected from any retaliation, threats, or attempts to retaliate against, in relation to your report. If, as a reporting person, you or any third-party person connected to you becomes the target of such retaliation, please notify the Contact Persons so that we can immediately assist.

- Exemption from liability for obtaining, accessing, and disclosing the information

You will not be held liable for obtaining or accessing the information reported unless it constitutes a criminal offence. You will not be held liable for the disclosure of information, provided that there were reasonable grounds for you to believe that the information was true, and that reporting was necessary to reveal the breach.

7. WHERE TO FIND MORE INFORMATION?

If you have any questions on how to report breaches and the protection of reporting persons, please get in touch with the Contact Persons listed in item 4 above.

Information on the reporting of breaches through external channels or through public disclosure can be obtained from the website of the National Integrity Agency, https://www.integritate.eu.

The Handbook was adopted on 01.09.2023.

IBM ROMANIA S.R.L.