Information clause for persons submitting reports of violations and persons participating in follow-up actions

Pursuant to Articles 13 and 14 of 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 (General Data Protection Regulation – GDPR, OJ EU L, 2016, No. 119), we inform that:

1. The Controller of your personal data is the Medical Research Agency with its registered office at ul. Chmielna 69, 00-801 Warsaw.
2. The Controller has appointed a Data Protection Officer, who can be contacted at the following address: iod@abm.gov.pl.
3. Your personal data will be processed for the purpose of receiving a report concerning violations at the Medical Research Agency, conducting follow-up actions, and possibly taking actions related to forwarding the report to the appropriate authorities.
4. Depending on the type of violations covered by the report, your personal data contained in the report will be processed on the basis of:
   a) Article 6(1)(c) GDPR in conjunction with the Act of 14 June 2024 on the protection of whistleblowers; processing is necessary to fulfill the legal obligation incumbent on the Medical Research Agency. Data processing is carried out in order to conduct follow-up actions concerning the violation at the Controller and possibly forward the report to the appropriate authorities,
   b) Article 6(1)(e) GDPR, for the purpose of the Controller performing tasks carried out in the public interest or in the exercise of public authority vested in the Controller under the provisions of the Act of 21 February 2019 on the Medical Research Agency.
5. Your personal data regarding your voice may be processed in the form of an audio recording via a recording device in order to conduct an investigation and prepare a report by the person conducting the investigation on the basis of Article 6(1)(e) GDPR; processing is necessary to perform a task carried out in the public interest, consisting in conducting the investigation and ensuring the correctness and reliability of follow-up actions, with particular regard to the protection of the personal data of the whistleblower, witnesses, and the person to whom the report relates.
6. During a direct meeting, with your consent, your oral report will be documented in the form of:
   a) a recording of the conversation, allowing for its retrieval, or
   b) a meeting protocol accurately reflecting its course, prepared by an authorized person.
7. Your personal data processed in connection with receiving the report or conducting follow-up actions, as well as documents related to this report, will be stored for a period of 3 years after the end of the calendar year in which the external report was forwarded to a public authority competent to take follow-up actions or after the follow-up actions were completed, or after the completion of proceedings initiated by these actions. Your personal data will be retained for archival purposes in accordance with the Filing Instructions and the Uniform File Classification Schedule or until any claims arising under legal provisions expire. Voice recordings made via a recording device for the purpose specified in point 5 will be deleted after the preparation of a service note or protocol.
8. Personal data were obtained:
   a) in the case of persons submitting reports of violations – directly from you,
   b) in the case of a person assisting in submitting a report of violations or the person to whom the report relates – from the person submitting the report of violations. The scope of your personal data necessary for identification may include: name and surname, position, workplace, contact details, and other data necessary in connection with verifying the report and conducting follow-

up actions, or indirectly from the person submitting the report. Information regarding the source of data may be limited in cases provided for in the above-mentioned Act.

9. Your personal data may only be disclosed to authorities or entities authorized under separate provisions or performing tasks carried out in the public interest or in the exercise of official authority. Personal data may also be disclosed by us to entities providing IT systems to the Controller, as well as providing IT tools, postal services, or document destruction services. In particular, your data may be transmitted to Whistleblowing Solutions AB, providing an IT tool for reporting violations – the Whistlelink system. The Whistlelink system protects the confidentiality and security of data. Access to such data is limited, and data principles and procedures aim to safeguard against loss, misuse, or disclosure. Data may also be transferred by Whistleblowing Solutions AB to subprocessors: Swerolab AB (Sweden), Interactive Security (Sweden), SMSAPI (Poland), Brevo (France), OPSWAT (Romania), Glesys (Sweden), T-Systems International (Germany), Friendly Captcha (Germany), DeepL (Germany), Mistral AI (France). Data are stored within the European Economic Area.
10. Your personal data will not be subject to automated decision-making, including profiling.
11. You have the right to request from the Controller access to your personal data, the right to rectification or restriction of processing, and the right to erasure. You also have the right to object to data processing, but this right applies only if further processing is not necessary for the Controller to fulfill a legal obligation and there are no overriding legal grounds for processing.
12. You have the right to lodge a complaint with the supervisory authority – the President of the Personal Data Protection Office.
13. Providing personal data is voluntary. Confirmation of receipt of the violation report and feedback regarding the matter will be provided via the reporting account in the Whistlelink system or to the contact address (if provided). Failure to provide personal data may hinder or prevent verification of the report and follow-up actions. Providing data within the scope required by the Whistleblower Act is mandatory.
14. Your personal data will not be transferred to a third country or an international organization.