Information Clause for Whistleblowers and Persons Involved in the Follow-up Actions

In accordance with Article 13 and 14 of the 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 119, 2016), we hereby inform that:

1. The Controller of your personal data is the Medical Research Agency (MRA), seated at ul. Chmielna 69, 00-801 Warsaw.
2. The Controller has appointed a Data Protection Officer whom you can contact at iod@abm.gov.pl.
3. Your personal data will be processed in order to receive the report of violations at the Medical Research Agency, to carry out the follow-up actions and possibly to take measures to forward the report to the relevant authorities.
4. Depending on the type of violations covered by the report, your personal data to the extent contained in the report will be processed on the basis of:
    a) Article 6(1)(c) of the GDPR, in connection with the Act of 14 June 2024 on the protection of whistleblowers; the processing is necessary for the fulfilment of a legal obligation incumbent on the Medical Research Agency. The processing is carried out in order to conduct the follow-up of the violation with the Controller and possibly to forward the report to the relevant authorities,
    b) Article 6(1)(e) of the GDPR; the Controller's performance of tasks in the public interest or in the exercise of public authority entrusted to the Controller under the provisions of the Act of 21 February 2019 on the Medical Research Agency.
5. Your personal data in relation to your voice may be processed in the form of an audio recording via a recording device for the purpose of the investigation and the preparation of the records by the investigator on the basis of Article 6(1)(f) of the GDPR, the legitimate interest of the correctness and fairness of the follow-up, with particular regard to the protection of the personal data of the whistleblower, witnesses and the reported person.
6. During the in-person meeting, with your consent, your verbal report is documented in the following form:
    a) a retrievable recording of the conversation, or
    b) minutes of the meeting, reproducing its exact proceedings, prepared by an authorised person.
7. Your personal data processed in connection with the acceptance of a report or taking the follow-up actions and the documents relating to that report shall be retained for a period of 3 years after the end of the calendar year in which the external report has been transmitted to the public authority competent to take the follow-up actions or in which the follow-up actions have been completed, or after the proceedings initiated by those actions have been concluded. Your personal data will be kept for archival purposes for a retention period in accordance with the Office Instructions and the Uniform Material List of Files or until the statute of limitations for possible claims under the law. Personal voice data recorded by means of a recording device for the purpose indicated in paragraph 5 will be deleted after minutes have been drawn up.
8. Personal data was obtained:
    a) in the case of whistleblowing reports submitted directly by you, your personal data has been obtained directly from you,
    b) in the case of a person assisting in the filing of a report of a violation and the reported person, the data has been obtained from the person filing the report of a violation. The scope of your personal data necessary for identification may include: your full name, position, place of work, contact details and other data necessary in connection with the verification of the report and the follow-up actions or indirectly from the person submitting the report of a violation. Information on the

source of the data may be restricted in the cases provided for in the aforementioned Act.

9. Your personal data may be made available only to bodies or entities authorised under separate regulations or performing tasks carried out in the public interest or in the exercise of public authority. Personal data may be shared by us with entities that operate the Controller's ICT systems and provide ICT tools, mail services or record destruction services. In particular, your data may be transferred to Ernst & Young spółka z ograniczoną odpowiedzialnością Consulting sp. k. providing an IT tool for reporting violations – EY VIRTUAL COMPLIANCE OFFICER ("VCO"). The VCO tool protects the confidentiality and security of data. Access to such data is restricted and data policies and procedures are designed to protect the data from loss, misuse or disclosure. Data may also be transferred by Ernst & Young spółka z ograniczoną odpowiedzialnością Consulting sp. k. to the Microsoft company providing Microsoft Azure cloud services for it. The Microsoft Azure cloud storage site is located in the Netherlands. Ernst & Young spółka z ograniczoną odpowiedzialnością Consulting sp. k. may transfer data to EY group companies.
10. Your personal data is not subject to automated decision-making, including profiling.
11. You have the right to demand from the Controller the access to personal data and the right to rectify them or limit their processing and to erase them. You also have the right to object to the processing of your data, but only if the further processing is not necessary for the fulfilment of a legal obligation by the Controller and there are no other overriding legal grounds for the processing.
12. You have the right to lodge a complaint with the supervisory authority – the President of the Office for Personal Data Protection.
13. The provision of personal data is voluntary. Acknowledgement of the receipt of the violation report and feedback on the case will be sent to the reporting account in the VCO tool or to the contact address (if provided). Failure to provide personal data may make it difficult or impossible to verify the report and carry out follow-up actions. The provision of data within the scope of the Whistleblower Act is mandatory.
14. Your personal data will not be transferred to a third country/international organisation.