DATA PRIVACY NOTICE FOR PATIENTS AND HEALTHCARE PROFESSIONALS FOR REPORTING ADVERSE EFFECTS

This data privacy notice details the rules applicable to processing personal data carried out by MSD Pharma Hungary Limited Liability Company (seat: HU-1095 Budapest, Lechner Odon fasor 10/B.; company reg. no.: Cg. 01-09-903998; tax no.: 14440791-2-44; hereinafter referred to as: "**MSD**" or "**Data Controller**") within the scope of adverse effect reporting.

Upon reporting any kind of adverse effect or side effect experienced in relation to using, applying or possessing any medicinal product of the company group of MSD Pharma Hungary Ltd., you help us comply with out statutory obligations and concurrently support us in the continuous monitoring and assessment of our products. Data processing in relation to adverse effect reporting is required by law, including especially Act XCV of 2005 on Medicinal Products for Human Use and on the Amendment of Other Regulations Related to Medicinal Products (hereinafter referred to as. "**Act on Medicinal Products**") and Decree 15/2012 (VIII. 22.) of the Ministry of Human Resources on the Pharmacovigilance of Medicinal Products for Human Use (hereinafter referred to as: "**Pharmacovigilance Decree**"). The Data Controller is obliged to investigate any and all reports involving a suspected adverse event, which comes from patients or healthcare service providers, either electronically or in any other manner allowing assessment. Possible adverse events can be reported in person, at the Data Controller's contact address set out in this Privacy Notice, or by means of filling out the online form available on the Data Controller's websites, or by means of e-mail, fax, sms or per telephone.

Data Controller fully observes and complies with applicable statutory provisions, including especially provisions of the European General Data Protection Regulation (hereinafter referred to as: "**GDPR**") within the scope of adverse effect reporting and in connection with any information disclosed thereunder.

Data Controller shall process personal data it receives in a confidential manner, in compliance with applicable statutory provisions and ensures the security of the personal data, including protection against loss, unlawful alteration or use by adopting appropriate technical and organizational measures and procedural rules. The personal data you disclose can only be accessed by persons engaged by the Data Controller, for them to be able to fulfil their tasks arising from their position and to the extent absolutely necessary to carry out such tasks. The Data Controller shall oblige all third persons to whom data can possibly be provided or transferred in compliance with prevailing statutory provisions to also ensure that such data security measures are taken.

PURPOSE, LEGAL BACKGROUND AND DURATION OF DATA PROCESSING

The Data Controller shall record all adverse events reported by patients or healthcare service providers or which it becomes aware of within the scope of the trials it conducts, in compliance with Point (c) of Article 6.1. and Point (i) of Article 9.2. of the GDPR and Sections 18(1)-(2) of the Act on Medicinal Products. The Data Controller must also report the adverse events it becomes aware of, i.e. it must transfer related data. The recipient of such transfer is the European Medicines Agency (6 Domenico Scarlattilaan, 1083 HS Amsterdam, the Netherlands), which stores data received within the scope of such reports in its system set up in compliance with Article 24 of Regulation (EC) no. 726/2004/EK (hereinafter referred to as: „**EudraVigilance System**"). Rules of the Pharmacovigilance Decree shall further govern the processing, storage and transfer of data.

In order to be able to efficiently investigate the circumstances of an adverse event, the Data Controller is entitled to transfer data to Merck & Co., Inc., Rahway, NJ, USA, its affiliates and other contractual partners of the Data Controller, both within the European Economic Area (hereinafter referred to as: "**EEA**"), as well as outside.

In case we transfer your personal data to a country outside the EEA, which is not considered by the European Commission to offer an adequate level of protection for personal data, we shall ensure that the data processing is subject to adequate safeguards, as required by the GDPR and the availability of effective legal remedies for data subjects. Upon transferring personal data between companies of the same corporate group from the EEA to the United States of America, MSD shall apply binding corporate rules adopted in accordance with Article 47 of the GDPR. Concurrently, the Data Controller shall comply with the requirements of the co-called "Data Privacy Framework Program" and furthermore, we shall at all times, if required, apply adequate contractual and other safeguards to ensure the protection of personal data in case we transfer personal data to our affiliates or external partners located in third countries.

For further information on data transfer to third countries, please refer to our Global Cross Boarder Privacy Rules Policy.

MSD can engage data processors to carry out certain data processing tasks in relation to the data processing carried out within the scope of adverse event reporting (for example to provide server hosting services and system administration services required for the operation of the website msd.hu). MSD currently engages the following data processors:

- Reflex Ltd. (seat: HU-3530 Miskolc, Szemere Bertalan u. 2. I. em. 107. ajt.; company reg. no.: 05-09-000445; tax no.: 10394863-2-05)

MSD reserves its right to change or amend the above list of data processors from time to time, however you can request information any time on data processors engaged and their availabilities from the Data Controller. MSD is responsible for ensuring that the data processors it engages fully comply with applicable statutory provisions pertaining to data protection at all times.

Data is processed by the Data Controller until it is required for its processing purpose or, if applicable, until deletion is requested. We hereby inform you however that the Data Controller has statutory obligations to store certain data pertaining to adverse event reports (for example the healthcare and other circumstances regarding the given adverse event) for an unlimited period of time, therefore the Data Controller may not be entitled to delete such data even in case of your explicit related request.

LEGAL BASIS FOR PROCESSING

Legal bases for data processing in relation to any side effects or adverse events your report are Section 18(1) of the Act on Medicinal Products and Sections 6(1) and 6(8) of the Pharmacovigilance Decree, in accordance with Point (c) of Article 6.1. and Point (i) of Article 9.2. of the GDPR. Considering the fact that the processing of data necessary for the effective and substantive investigation of the report stems from the Data Controller's legal obligation, the data processing carried out in this regard is not dependent on your consent.

The processing of any data you provide within the scope of the report that is not necessary for the substantive investigation of the report is based on your consent, in accordance with Point (a) of Article 6.1. of the GDPR.

Your consent is freely given and – with the exception of data necessary for the effective and substantive investigation of the adverse even report – can be withdrawn any time. Please note however that certain data may be processed further despite the withdrawal of your consent, if they are required by the Data Controller to enforce its legitimate interest.

CATEGORIES OF PERSONAL DATA CONCERNED

The Data Controller shall store and process the personal data you provide within the scope of adverse event reporting, including especially (i) the initials of the patient, (ii) the patient's age or year of birth, (iii) the patient's sex, (iv) the health related data pertaining to the reported adverse event, or related data pertaining to a person's physical condition, (v) contact data of the person making the report (either the patient or the healthcare service provider), including specifically their name, telephone number, fax number, postal address, e-mail address, their profession or workplace.

In case you provide personal data other than your own within the scope of adverse event reporting, please always make sure to notify the given person of their data you intend to report before making the report.

YOUR RIGHTS IN RELATION TO THE DATA PROCESSING

In accordance with Hungarian and EU statutory provisions pertaining to data protection you have the right to:

- receive confirmation / feedback of whether or not your personal data is being processed, and if it is, you are entitled to request access to your personal data. Within such scope **you can receive especially the following information**: the purposes of processing, the categories of personal data processed, the recipients or categories of recipients to whom personal data has been or will be disclosed (Article 15 of the GDPR);

- have the Data Controller provide you with a copy of your personal data;

- request the **rectification** of your inaccurate personal data or have your incomplete personal data **completed** (Article 16 of the GDPR);

- request the **erasure** (deletion) of your personal data in cases specified by the GDPR (for example if you withdraw your consent on which the processing is based or your personal data is no longer necessary in relation to the purposes of data processing) (Article 17 of the GDPR);

- request the **restriction of the processing** of your personal data in cases specified by the GDPR. You can be entitled to restrict the processing of your personal data if you contest the accuracy of your personal data processed by MSD, or you object to the processing of your personal data or if MSD processes your personal data unlawfully and you request the restriction of processing instead of the erasure of your data. You are also entitled to exercise the right to restrict your data if MSD no longer needs your personal data for the purposes of the processing, but you require it for the establishment, exercise or defense of legal claims. If you have requested the restriction of the processing of your personal data in the above manner, the data concerned can only be further processed (beyond its storage) within the narrow scope specified by the GDPR (for example if the personal data affected by the restriction is required to exercise legal claims) (Article 18 of the GDPR);

- exercise your **right to data portability** by requesting MSD as Data Controller to provide you with your personal data in a structured, commonly used and

machine-readable format or to transmit such data to another controller. You have the right to data portability if the processing is based on your consent or on the performance of a contract which you are a party to, and – in both cases – if the processing is carried out by automated means (for example within the scope of a computer system) (Article 20 of the GDPR).

MSD may refuse to comply with your data access or data correction request if one of the following is true:

- MSD is not processing the information in question.
- MSD has not been provided with enough information to:
  - confirm the identity of the requestor. (if, for example MSD only has direct access to pseudonymized/coded data). Within such scope MSD may use all reasonable measures to verify the identity of a data subject who requests access. Where applicable, MSD may forward the request and/or refer the data subject to a party able to respond to the data subject's request;
  - locate the personal data;
  - confirm that the personal data to which the data correction request relates is inaccurate, incomplete, misleading or not up to date.
- The burden and expense of providing access is disproportionate to the risk to the person's privacy.
- MSD is unable to comply with the data access request without disclosing personal data relating to another individual who can be identified from that information.
- Another data controller uses the personal data to which the data access request relates in such a way as to prohibit MSD from complying.
- Providing access would:
  - be a violation of a court order;
  - disclose confidential commercial information; or
  - access to personal data is regulated by another law.

The Data Controller shall use its best endeavors to comply with data protection related requests. However in accordance with the GDPR, it may refuse to delete data that is absolutely necessary for the Data Controller to be able to comply with its legal obligations or to enforce its legitimate interests.

CONTACT DATA

If you would like to enforce your above rights, or have any questions or comments regarding this notice or our data processing activities, visit the MSD company group's website on our commitment to privacy or turn to us through one of the following availabilities:

MSD Pharma Hungary Ltd.:
Seat: HU-1095 Budapest, Lechner Odon fasor 10/B.

E-mail address: hungary_msd@msd.com
Telephone number: +36 (1) 888 5300

You can also contact MSD Pharma Hungary's data protection officer at:
dpohungary@msd.com

We hereby inform you that we can only provide general information per telephone, so please submit all further, specific requests either in writing or per e-mail in order for us to be able to verify your identity, if necessary.

MSD shall make efforts to answer or address your data protection related requests as soon as possible, but within one (1) month upon receipt at the latest. Please note however that in accordance with the GDPR, MSD may be entitled to extend this deadline by a further two (2) months if this is necessary due to the complexity and/or large number of requests submitted by you. We shall inform you of any such extension within one (1) month of receipt of the request.

If your request is not justified, therefore MSD cannot take action on your request, we shall inform you of this latest within one (1) month of receipt of the request (including information on the reasons for our refusal).

LEGAL REMEDIES

If you believe that your rights have been violated, you have the following options:

- contact the Data Controller directly via the contact details specified in this Privacy Notice;

- lodge a complaint with any of the supervisory authorities (for example in Hungary with the Hungarian National Authority for Data Protection and Freedom of Information, hereinafter referred to as: "**NAIH**"). Contact details of NAIH: seat: H-1055 Budapest, Falk Miksa utca 9-11.; PO box: H-1363 Budapest, Pf.: 9.; Telephone: +36-1-391-1400; e-mail: ugyfelszolgalat@naih.hu;

- initiate an action before court if you believe that your personal data has been processed unlawfully or in breach of data security requirements. In this case you can be entitled to damages or a grievance award. See the competences and contact details of the courts on the following website: www.birosag.hu.

In order to have your issues and observations relating to data processing resolved in the fastest and most effective manner, we recommend that you contact us first with any privacy-related request.

DATA SECURITY

MSD will take every reasonable measure to ensure the safety of your personal data at the highest level possible and will within such scope take every necessary technical and organizational measure and develop the required procedural rules to protect the personal data processed by MSD from unauthorized access, disclosure, alteration and erasure.

In accordance with the above, during the course of the entire process of data processing MSD:

- has implemented a comprehensive information security program and applies security controls that are proportional to the sensitivity of the information and the risk associated with the given data processing activity;

- takes into account the current technology best practices and the cost of implementation when developing the aforementioned mechanisms; and

- applies the following procedures and the related technical background in order to provide the necessary data security guarantees:

    - ensuring business continuity and data restorability;
    - taking appropriate encryption measures and restricting access to data;
    - preventing and managing data breaches;
    - guaranteeing the security of the online access to the data;
    - guaranteeing the security of the physical access to data carriers and other the documents;
    - performing continuous risk analysis and risk management related to data processing.

UPDATING THIS PRIVACY NOTICE

The Data Controller may amend this Privacy Notice – primarily in order to comply with any amended statutory requirements, including especially any amendments to the GDPR – in the future. The Data Controller reserves its right to change, amend or delete certain parts of this Privacy Notice at its own discretion. We recommend that you review this Privacy Notice from time to time to ensure that you are up to date regarding all facts and information contained therein.

This Privacy Notice was last updated on August 4, 2026.