Information to the data subjects on personal data protection and exercise of rights in relation to complaints processed locally in Spain in the Novartis Internal Information System (SpeakUp).

Data controller and data protection officer contact details

The data controller is Novartis International AG, Basel, Switzerland. If you have any questions about your personal data or if you wish to exercise your data privacy rights, please contact privacy.switzerland@novartis.com or dpospain.novartis@novartis.com.

Purposes of the processing for which personal data are intended and recipients of the personal data

Personal information collected through this channel is used solely for the purpose of receiving and investigating reports of possible misconduct by Novartis associates.

Legal basis for processing

The processing of personal data, in cases of internal communication, shall be deemed lawful by virtue of the fact that it is mandatory to have an internal information system - the processing is necessary for the fulfillment of a legal obligation.

The processing of personal data deriving from a public disclosure shall be presumed to be for the performance of a task carried out in the public interest or in the exercise of public authority vested in the controller.

The processing of special categories of personal data for reasons of essential public interest may be carried out in accordance with the provisions of Article 9(2)(g) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR).

Processing of Personal Data in the Internal Information System

Communications may be submitted in writing or verbally. In these cases - by telephone, the informant will be warned that the communication will be recorded and that if he/she does not wish to allow it, he/she may report it by other means. He/she will also be informed of the processing of his/her personal data.

The identity of the informants and those who make a public disclosure shall in any case be kept confidential and shall not be communicated to the persons to whom the facts reported refer or to third parties.

The person to whom the reported facts refer shall in no case be informed of the identity of the informant or of the person who has made the public disclosure.

Internal reporting channels will even allow for the submission and subsequent processing of anonymous communications.

Personal data will not be collected if it is manifestly not relevant to the processing of specific information or, if collected by accident, will be deleted without undue delay.

Likewise, any personal data that may have been communicated and that refer to conduct that is not included in the scope of application of the law will be deleted.

If the information received contains personal data included in the special categories of data, it will be immediately deleted, without the registration and processing of such data.

Period during which personal data will be stored

The data processed may be kept in the information system only for the time necessary to decide whether to initiate an investigation into the reported facts.

If it is proven that the information provided or part of it is not truthful, it will be immediately deleted as soon as such circumstance comes to light, unless such lack of truthfulness may constitute a criminal offense, in which case the information will be kept for the necessary time during the legal proceedings.

After three months have elapsed since receipt of the communication without any investigation having been initiated, it is deleted, or anonymized - in order to leave evidence of the operation of the system.

Personal data is only kept for the necessary and proportionate period and, in no case, for a period longer than ten years.

Access to personal data contained in the Internal Information System

They are the people who access personal data:

- The person in charge of the system and whoever manages it directly
- The human resources manager or the duly designated competent body, only when disciplinary measures may be taken against an employee.
- The person in charge of the legal services, if legal action should be taken in relation to the facts described in the communication
- The persons in charge of the processing that may be appointed from time to time
- The data protection officer

The processing of data by other persons, or even their communication to third parties, will be lawful when necessary for the adoption of corrective measures in the entity or the processing of sanctioning or criminal proceedings that, where appropriate, may be applicable.

The identity of the informant may also be communicated to the judicial authority, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, disciplinary or disciplinary investigation. The informant shall be informed before his or her identity is revealed, unless such information could compromise the investigation or the judicial proceedings. When the competent

authority informs the informant, it shall send him/her a letter explaining the reasons for the disclosure of the confidential data concerned.

Likewise, the extension of confidentiality is guaranteed with respect to communications made through channels or persons other than those provided for in the information system, and Novartis personnel are expressly trained in this matter. Indeed, the Novartis Code of Conduct guarantees confidentiality and the prohibition of retaliation for whistleblowers in good faith.

Exercise of rights

Data subjects may exercise the rights referred to in Articles 15 to 22 of the GDPR - right of access, right of rectification, right of erasure ("the right to be forgotten"), right to limitation of processing, right to data portability and right to object, by sending an email to privacy.switzerland@novartis.com or dpospain.novartis@novartis.com. They may also exercise the right to lodge a complaint with a supervisory authority - Spanish Data Protection Agency.

Where processing is based on consent, there is a right to withdraw consent at any time, without affecting the lawfulness of processing based on consent prior to its withdrawal.

In the event that the person to whom the facts related in the communication or to whom the public disclosure refers exercises the right to object, it will be presumed that, unless proven otherwise, there are compelling legitimate grounds that legitimize the processing of his or her personal data.

Security and confidentiality measures

The internal information system has adequate technical and organizational measures to preserve the identity and guarantee the confidentiality of the data corresponding to the persons concerned and to any third party mentioned in the information provided, especially the identity of the informant in case he/she has been identified.