

Novartis – General Privacy Notice for Patients

April 2020

This Privacy Notice is addressed to our patients.

You are receiving this Privacy Notice because Novartis is processing information about you which constitutes “**personal data**” and Novartis considers the protection of your personal data and privacy a very important matter.

Novartis is responsible for the processing of your personal data as it decides why and how it is processed, thereby acting as the “**controller**”. In this Privacy Notice, “**we**” or “**us**” refers to Novartis.

We invite you to carefully read this Privacy Notice, which sets out in which context we are processing your personal data and explains your rights and our obligations when doing so.

Should you have any further question in relation to the processing of your personal data, we invite you to contact dsgvo.de@sandoz.com.

1 What information do we have about you?

We collect your general and identification information (e.g. name, first name, last name, gender, date and place of birth, email and/or postal address, fixed and/or mobile phone number).

Please note that we will not knowingly collect, use or disclose personal data from a minor under the age of 14 without obtaining prior consent from a parent or legal guardian.

2 For which purposes do we use your personal data and why is this justified?

2.1 Legal basis for the processing

We will not process your personal data if we do not have a proper justification foreseen in the law for that purpose. Therefore, we will only process your personal data if:

- we have obtained your prior consent;
- the processing is necessary to perform our contractual obligations towards you or to take pre-contractual steps at your request;
- the processing is necessary to comply with our legal or regulatory obligations;
- the processing is necessary to protect your vital interests or those of another person; or
- the processing is necessary for our legitimate interests and does not unduly affect your interests or fundamental rights and freedoms.

Please note that, when processing your personal data on this last basis, we always seek to maintain a balance between our legitimate interests and your privacy. Examples of such ‘legitimate interests’ are data processing activities performed:

- to benefit from cost-effective services (e.g. we may opt to use certain platforms offered by suppliers to process data);
- to offer our products and services to our customers;

- to prevent fraud or criminal activity, misuses of our services and products as well as the security of our IT systems, architecture and networks;
- to sell any part of our business or its assets or to enable the acquisition of all or part of our business or assets by a third party; and
- to meet our corporate and social responsibility objectives.

2.2 Purposes of the processing

We always process your personal data for a specific purpose and only process the personal data which is relevant to achieve that purpose. In addition to the specific purposes identified on the first two pages, we also process your personal data for the following general purposes:

- manage patients' data;
- for pharmacovigilance purposes (tracking of side effects);
- improve our products and services;
- research, development and commercialization of products;
- scientific research purposes or statistical purposes subject to appropriate safeguards such as pseudonymisation;
- training or educational purposes within or outside Novartis;
- provide you with adequate and updated information about disease, drugs, as well as our product and services;
- organize patients support or assistance programs (including connecting you with health resources and patients associations upon your request) and patients testimonials;
- answer any questions or requests you may have;
- manage our IT resources, including infrastructure management and business continuity;
- preserve the company's economic interests and ensure compliance and reporting (such as complying with our policies and local legal requirements, tax and deductions, managing alleged cases of misconduct or fraud, conducting audits and defending litigation);
- manage mergers and acquisitions involving our company;
- archiving and record-keeping; and
- any other purposes imposed by law and authorities.

3 Who has access to your personal data and to whom are they transferred?

We will not sell, share, or otherwise transfer your personal data to third parties other than those indicated in this Privacy Notice.

In the course of our activities and for the same purposes as those listed in this Privacy Notice, your personal data can be accessed by, or transferred to the specific third parties identified

in Part I above and to the following categories of recipients, on a need to know basis to achieve such purposes:

- our personnel (including personnel, departments or other companies of the Novartis group);
- our suppliers and services providers that provide services and products to us;
- our IT systems providers, cloud service providers, database providers and consultants;
- any third party to whom we assign or novate any of our rights or obligations; and
- our advisors and external lawyers in the context of the sale or transfer of any part of our business or its assets.

The above third parties are contractually obliged to protect the confidentiality and security of your personal data, in compliance with applicable law.

Your personal data can also be accessed by or transferred to any national and/or international regulatory, enforcement, public body or court where we are required to do so by applicable law or regulation or at their request.

The personal data we collect from you may also be processed, accessed or stored in a country outside the country where Novartis is located, which may not offer the same level of protection of personal data.

If we transfer your personal data to external companies in other jurisdictions, we will make sure to protect your personal data by (i) applying the level of protection required under the local data protection/privacy laws applicable to Novartis, (ii) acting in accordance with our policies and standards and, (iii) for Novartis located in the European Economic Area (i.e. the EU Member States plus Iceland, Liechtenstein and Norway, the "EEA"), unless otherwise specified, only transferring your personal data on the basis of standard contractual clauses approved by the European Commission. You may request additional information in relation to international transfers of personal data and obtain a copy of the adequate safeguard put in place by exercising your rights as set out in Section 6 below.

For intra-group transfers of personal data to our group companies (which you can identify by clicking this link https://www.novartis.com/our-company/contact-us/office-locations?tid=All&name_list=DE, the Novartis Group has adopted Binding Corporate Rules, a system of principles, rules and tools, provided by European law, in an effort to ensure effective levels of data protection relating to transfers of personal data outside the EEA and Switzerland. Read more about the Novartis Binding Corporate Rules by clicking here <https://www.novartis.com/privacy-policy/novartis-binding-corporate-rules-bcr>.

4 How do we protect your personal data?

We have implemented appropriate technical and organisational measures to provide an adequate level of security and confidentiality to your personal data.

These measures take into account:

- (i) the state of the art of the technology;
- (ii) the costs of its implementation;
- (iii) the nature of the data; and

(iv) the risk of the processing.

The purpose thereof is to protect it against accidental or unlawful destruction or alteration, accidental loss, unauthorized disclosure or access and against other unlawful forms of processing.

Moreover, when handling your personal data, we:

- only collect and process personal data which is adequate, relevant and not excessive, as required to meet the above purposes;
- ensure that your personal data remains up to date and accurate (for the latter, we may request you to confirm the personal data we hold about you. You are also invited to spontaneously inform us whenever there is a change in your personal circumstances so we can ensure your personal data is kept up-to-date); and
- process any sensitive data about yourself (including your medical/health related data) you provide in compliance with applicable data protection rules and strictly as required for the relevant purposes listed above. The data is accessed and processed solely by the relevant personnel, under the responsibility of one of our representatives who is subject to an obligation of professional secrecy or confidentiality.

5 How long do we store your personal data?

We will only retain your personal data for as long as necessary to fulfil the purpose for which it was collected or to comply with legal or regulatory requirements.

The retention period is set out at the beginning of this Privacy Notice. When this period expires, your personal data is removed from our active systems.

6 What are your rights and how can you exercise them?

You may exercise the following rights under the conditions and within the limits set forth in the law:

- the right to access your personal data as processed by us and, if you believe that any information relating to you is incorrect, obsolete or incomplete, to request its correction or updating;
- the right to request the erasure of your personal data or the restriction thereof to specific categories of processing;
- the right to withdraw your consent at any time, without affecting the lawfulness of the processing before such withdrawal;
- the right to object, in whole or in part, to the processing of your personal data; and
- the right to request its portability, i.e. that the personal data you have provided to us be returned to you or transferred to the person of your choice, in a structured, commonly used and machine-readable format without hindrance from us and subject to your confidentiality obligations.

If you have a question or want to exercise the above rights, you may send an email to dsgvo.de@sandoz.com with a scan of your identity card for identification purpose, it being understood that we shall only use such data to verify your identity and shall not retain the

scan after completion of the verification. When sending us such a scan, please make sure to redact your picture and national registry number or equivalent on the scan.

If you are not satisfied with how we process your personal data, please address your request to datenschutz@novartis.com or send a letter at Novartis Business Services GmbH, Datenschutzbeauftragter, Industriestraße 25, 83607 Holzkirchen.

In any case, you also have the right to file a complaint with the competent data protection authorities, in addition to your rights above.

7 How will you be informed of the changes to our Privacy Notice?

Any future changes or additions to the processing of your personal data as described in this Privacy Notice will be notified to you in advance through an individual notice through our usual communication channels (e.g. by email or via our internet website).