NOVARTIS

Data Privacy Policy

Novartis Global Data Privacy Policy

Effective: September 1, 2020

Version: V3.1.EN Public

Group Data Privacy

Contents

1 Introduction

1.1 Purpose

At Novartis, and as reflected in our Code of Ethics, we are committed to the responsible use of Personal Information in our business processes and the setting of the appropriate standards to achieve this purpose. To that end, we have developed the following privacy principles to be applied to the Processing[1] of Personal Information in daily activities by all Novartis Associates.

1.2 Scope and Applicability

This Policy applies to all Novartis Associates as well as to all Processing of Personal Information on behalf of Novartis. Each Associate is accountable for compliance with Data Privacy obligations.

This Policy sets the global privacy standards for Novartis. In addition, all Processing of Personal Information must be conducted in accordance with relevant local laws, regulations and industry codes, which may be more stringent than the requirements outlined in this Policy.

Associates manage Personal Information entrusted to Novartis by patients, consumers, healthcare professionals, customers, employees and others on a daily basis. For example:

	EXAMPLES OF PROCESSING ACTIVITIES
Finance & Procurement	Associates' Personal Information for the management of expense reports or cost centers. Vendor and spend data, contracts and assessments managed by Procurement
People & Organization	Employee benefit programs, pay, talent management, and recruitment activities. Associates' Personal Information for the management of Personnel administration, performance review, and workplace monitoring
Marketing, Medical	Market Research, development and provision of programs such as Patient Support Programs, social media listening, email communications, newsletters, mobile applications, other digital platform, and analytics
Sales	Interactions and communications with Healthcare Professionals to establish and maintain effective relationships
Medical	Engagement of Healthcare Professionals, scientific experts and Key Opinion Leaders for medical education program development, medical conferences and other events
Market Access	Conducting health outcome analysis with assistance of patient-derived Personal Information
Communications	Interactions with patients
Clinical Operations	Clinical trials and studies

[1] Means any activity, such as collection, use, storage, and sharing of Personal Information; see attached Privacy Glossary for complete definition

Research	Early development of new medicines, biomarkers and innovations using human biological samples, genetic data or data from clinical trials and/or biobanks

The owner of this Policy is the Group Data Privacy function.

2 Definitions

Please see the attached Privacy Glossary for the definitions of capitalized terms in this Policy.

3 Principles

Data Privacy is receiving increased societal attention and scrutiny, it is an emerging field of law with varying local maturity and evolving interpretation by the courts. We therefore need to apply a *principles based approach* to our decision making.

All Processing of Personal Information shall comply with the 5 fundamental principles as set out below. The 5 principles are embedded in our commitment to abide by a high standard of ethical business conduct:

Principle 1 – Transparency

Principle 2 – Legitimate and Meaningful Collection

Principle 3 – Responsible and Sustainable Processing

Principle 4 – Security, Integrity and Quality

Principle 5 – Minimal Retention

At the back of each principle examples are given to illustrate how the principles can be generally applied - please note that, depending on the context, other mandatory elements may need to be considered.

3.1 Principle 1 – Transparency

We are transparent about what Personal Information we Process, how and why we collect it, use it, and who we share it with. We explain this in clear and simple language.

3.1.1 Background

A fundamental principle of Data Privacy is that organizations must be open and transparent about how they manage the Personal Information they are entrusted with. This important principle both enhances our accountability for our practices in handling Personal Information and builds trust and confidence in these practices amongst our associates, vendors, customers, HCPs, patients and stakeholders.

3.1.2 Implementation

Associates must:

- Provide information to Individuals about how their Personal Information will be used by Novartis at the time we collect the Personal Information (if practicable), or as soon as possible afterwards. This can be communicated in different ways, such as by providing Privacy Notices, Consent forms and/or privacy policies, on websites, or in printed materials when appropriate. Regardless of the form it takes, the information provided should be concise, transparent and written in clear and plain language.

- Consider referring to the general Novartis Privacy Statement on the Novartis corporate websites regarding the use of Personal Information. It may need to be complemented with an individual specific notice, depending on the activity and/or local legal or regulatory requirements.

- Focus on what is important for the Individual to know, and provide specifics about the handling of and type of Personal Information. The information should accurately and completely reflect the actual use of the data. For example, a notice for the collection of Sensitive Personal Information, such as health information, is likely to be more detailed than a notice on the collection of contact information. Your Data Privacy Business Partner can help you develop a notice appropriate to the circumstances.

3.1.3 Examples

Privacy Notice provided to Clinical Trial Patients

Everyone taking part in a clinical trial must be given information about the key aspects of the trial.

Clinical trials generally involve the Processing of Sensitive Personal information of Individuals and so Novartis provides detailed information to participants to help them decide whether to take part in the trial or not.

Information is provided to participants on the conduct of the clinical trial, details on what Personal Information is likely to be collected, such as contact information as well as biological samples that could identify the Individual, and information related to their particular disease or condition.

Personal Information may be sent overseas so the participant is given information that their Personal Information may be sent outside of the country in which it was collected.

Full information about how the participants Personal Information is used is provided to them in a Privacy Notice, which is usually part of an Informed Consent Form.

Privacy Notice provided to Healthcare Professionals

Novartis is considering developing an external website in a country for Healthcare Professionals to access exclusive content from experts, watch videos and learn about new products. In order to register for access to the Novartis website, HCPs will need to provide some basic contact information to set up an account. A Privacy Notice is provided to the HCP at the point they provide their information so they understand how their Personal Information will be used.

3.2 Principle 2 – Legitimate and Meaningful Collection

We connect all collection and use of Personal Information to specific business purposes related to how we operate, innovate or engage.

3.2.1 Background

We will only collect Personal Information if we have specific and legitimate reasons or requirements to do so. We only collect the minimum amount necessary for specific purposes. By not collecting more data than is required or needed we reduce the risks related to the Processing of the Personal Information. By limiting our collection to specific purposes we demonstrate a responsible use of the Personal Information entrusted to us.

3.2.2 Implementation

Associates must:

- Identify the business objective and legitimate reason for collecting Personal Information. Your Data Privacy Business Partner can advise on the legal grounds for the collection of Personal Information.
- Explore whether alternatives to collecting Personal Information may be available to meet the specific purpose.
- Ensure that the Processing of Personal Information is only done to meet the identified business objective and legitimate reason (e.g., a legal requirement to manage handling of adverse events).
- Only collect the minimum amount of Personal Information needed for the specific purpose.
- Understand and recognize that there may be additional Data Privacy requirements when Processing Sensitive Personal Information.

3.2.3 Examples

Patient Information in a Digital Application

Novartis develops digital applications (“apps”) for patients who could benefit from improving the management of their disease. These apps may have a variety of features, depending on the disease, treatment and the needs of the patient, and the business needs of Novartis; from monitoring and tracking symptoms, to providing patients with reminders on their medication regimen or medical appointments, to tracking app usage through analytics. The technology can allow for patient data to be shared with third parties: a caregiver, a parent/legal guardian, a healthcare professional (e.g., a nurse, family physician, and specialist).

When developing such patient apps, legitimate and meaningful collection means that we must carefully consider the purposes for which we collect Personal Information: how will the app use the Personal Information and in what ways? If the purpose for collection is defined too narrowly, we may be unable to use the information in the ways we would like. For example if the purpose of the app is defined as exclusively assisting patients with taking their medication on time, we must not collect any additional information on how patients feel or to help them track their symptoms.

If the purpose is defined too broadly we risk collecting information for which we have no business justification. For example, if we defined the purpose as ‘helping patients with

their condition' this does not adequately explain how a patient's Personal Information will be used. Having clearly defined purposes makes it easier for us to identify which Personal Information needs to be collected and for which specific purposes, to put in place the appropriate safeguards, to describe our objectives in plain language and to be transparent to our stakeholders.

EXAMPLE: Novartis has developed an easy to use app for a smartphone or mobile device for patients to use. The purpose of the app is to help patients keep track of their symptoms and enhance the management of their disease. No Personal Information or data analytics are collected by Novartis. App users are advised that Personal Information related to the *features of the app* remain solely on their smart phones or devices and are not shared with Novartis.

People & Organization Processing Associates' Personal Information

Human Resources in a country wants to provide a weather alert service to associates and Third Party contractors with a 5-2-1 ID, to advise them in case of office closure due to adverse weather conditions. This service is offered via a Third Party provider specializing in such notification services. To deliver the service, the Third Party provider will request that each associate or Third Party contractor register on their website and provide their email, a telephone number, address and gender. As an address or gender is not required to provide this service, HR requests the Third Party provider to remove these data fields from the registration page.

Finance Processing Associates' Personal Information

Finance wishes to develop reports involving associate Personal Information, such as first and last name, salary, bonus, expenses and travelling details. These reports have an identified business purpose: managing the workforce and related costs.

Finance in a country may be required or asked by the global finance function to develop expense reports analysis along with cost centers or bonus allocations. Prior to gathering this information, the local country and Global Finance should together determine what Personal Information of the associate is needed to develop a meaningful analysis and report. While an individual expense report will likely require Personal Information such as the first and last name of an associate, an expense report analysis based on combined expense reports (such as a report to determine total costs of travelling per organization) will probably not require the full name of an associate. By only Processing the minimum amount of Personal Information required, we reduce the risk of collecting additional, unnecessary information.

3.3 Principle 3 – Responsible and Sustainable Processing

We use Personal Information only in ways compatible with the purposes for which it was collected. We facilitate Individuals to exercise their rights with regards to their Personal Information.

3.3.1 Background

Responsible management of Personal Information is required to protect privacy rights and comply with Data Privacy laws. This includes ensuring that we only Process Personal Information we have collected for the original purposes for which it was collected, or for secondary uses that are appropriate. In doing so, we will meet our Data Privacy obligations and strengthen the trust of Individuals who entrust us with their data.

3.3.2 Implementation

Associates must take appropriate steps to:

- Use Personal Information only for specific business purposes described in the Privacy Notice, with specific legitimate justifications.

- Ensure that if Personal Information is collected for particular purposes, it can only be used for an additional secondary purpose if there is a legitimate justification. Such justification may include, where allowed, the conduct of a compatibility test, the collection of additional Consent from the Individual, or the applicability of additional safeguards, such as Pseudonymization. Before any secondary use of information, such as for research and statistical purposes, associates must seek advice from their Data Privacy Business Partner.

- Prevent the use of Personal Information for a purpose that is not compatible with the original purpose it was collected for, or another legitimate secondary purpose.

- Discuss with your Data Privacy Business Partner before you share Personal Information with Third Parties.

- Obtain assurances from third parties who Process Personal Information on Novartis' behalf that they have the ability and intention to protect Personal Information to the appropriate standard in accordance with this Policy and local data privacy requirements. This assurance could take the form of a contract which includes relevant Data Privacy terms and Processing instructions.

- Follow relevant local procedures for any legal requirements when transferring Personal Information across country borders. We have implemented mechanisms which in most circumstances allow internal data transfers of Personal Information within Novartis. Associates may need to provide specific notice to the Individuals whose Personal Information is being transferred, and in certain cases the transfer may require their Consent. In some instances we may also need to notify a local data protection authority, or put in place contractual safeguards to protect the Personal Information. Your Data Privacy Business Partner will support you in assessing and reviewing any risks relating to such sharing.

- Take into account these privacy principles at all stages when developing and designing products, services and applications and ensure that, by default, only Personal Information which are necessary for each specific purpose of the Processing are being Processed.

- Consult your Data Privacy Business Partner when Personal Information is Processed which is leading to an automated decision that affects an Individual.

- Implement or apply existing processes to ensure an appropriate and lawful response is given to Individuals who wish to exercise their legal rights (*e.g.*, access, or deletion). Associates should consult their Data Privacy Business Partner to understand what rights are applicable in their country, and to discuss how to facilitate the exercise of these rights.

3.3.3 Examples

Patient Focus Group

In a country, the Communication and Patient Advocacy Team has conducted patient focus groups in collaboration with a local patient association to understand the challenges of patients living with breast cancer. The focus groups are organized and managed by a Third Party agency. The patients are recruited by the patient association who has reached out to its members to identify patients with an interest.

Each patient signs a Consent form to participate in the focus group and is advised that their data will be Processed by the Third Party agency who will anonymize the results prior to sharing with Novartis. The focus groups are a success and provide helpful information on breast cancer patients' journeys. In the final report sent to Novartis, the agency makes a suggestion that the patients may be potential candidates for an upcoming Novartis clinical trial assessing the safety and efficacy of a new breast cancer treatment. The agency suggests that Novartis keeps the patient information in order to contact them in a few months to validate their interest. The Novartis team advises the Third Party that the Consent does not address this purpose and therefore Novartis cannot reach out to these patients, directly or indirectly for this new purpose.

Correcting inaccurate Personal Information

A new associate receives their pay slip for the previous month and notices an error that her home address is no longer up to date. The associate contacts her HR function and informs them that she recently moved and the address on file is no longer accurate. HR follows the appropriate process, and corrects the information on the associate's employment file so that the associate's new address is accurately recorded across all relevant HR systems.

Adverse Events

Many adverse events which are reported to Novartis are handled in the Novartis Global Service Center in India. In order to allow this Processing, Novartis has ensured that a Data Processing Agreement has been entered into to permit the transfer of data between the different Novartis legal entities in the various countries. Novartis provides notice to patients and healthcare professionals that the management of adverse events may occur in a country other than their country of residence.

3.4 Principle 4 – Security, Integrity and Quality

We protect Personal Information by using reasonable safeguards to prevent its loss, unauthorized access, use, alteration or unauthorized disclosure, and take appropriate steps to keep Personal Information accurate and up to date.

3.4.1 Background

Novartis is entrusted with Personal Information and is responsible for taking reasonable steps to protect that information from misuse, interference and loss, as well as unauthorized access, modification or disclosure.

The nature of the Personal Information, and the risk of a security incident occurring, will guide the level of protection. Sensitive Personal Information requires a higher standard of protection. Information Security Risk Management ('ISRM') policies and standards include more information on the classification of information, and should be taken into account when assessing appropriate levels of information security. Security measures may be physical, such as locks and access cards for buildings, electronic, such as encryption and passwords, or organizational, such as restricting access to information to only those who need it. To ensure the initial accuracy of data and to maintain its integrity and quality, we need to regularly verify that the information is accurate and up to date.

3.4.2 Implementation

Associates must:

- Take appropriate steps to keep Personal Information accurate and up to date through the information lifecycle, i.e. from collection through to destruction. For example, Individuals could be provided with a simple means to review and update their Personal Information on an on-going basis, and new or updated Personal Information is promptly added to a relevant record or Database.

- Safeguard Personal Information so that it is not shared with others who do not have a valid business reason to access the information (sometimes referred to as a 'need to know' rule). For example, there would likely not be a valid reason for identifiable clinical research data to be shared with marketing associates for marketing purposes.

- Report any actual or suspected Personal Data Security Incident, including loss or unauthorized access, to the IT Service Desk.
- Comply with Novartis Information Security policies and guidelines when Processing Personal Information such as implementing encryption, restricted-access to electronic folders and restricted-access rooms, applying a clean desk policy and securely destroying documents. Additional organizational or technical safeguards should also be considered.

- Consider, with the assistance from their Data Privacy Business Partner, whether to Anonymize or Pseudonymize (see definitions in the attached Privacy Glossary) the Personal Information as an appropriate security measure.

3.4.3 Examples

Disease Awareness Website

A local Novartis organization has set up a disease awareness website where visitors may register to receive newsletters providing information on the disease and management of the disease. To register for the newsletter, website visitors are asked to provide their first name and email address. The email address is to be able to send the electronic newsletter and the first name is to personalize the communications. The data will be stored in an internal Novartis Database. In addition to having an appropriate notice and legal basis for the Processing, the team consults Data Privacy and ISRM to make sure that this data is stored on a secure platform with the appropriate safeguards, and completes the electronic Privacy Assessment (ePA) process to assess the potential privacy risks.

Accidental Disclosure

In order to provide employees with regular information on their pay, a local Novartis entity has implemented an internal web platform where each employee can view their own salary statements. A technical error occurs and when accessing the platform this week, you realize that you can view salary statements of other employees in your country. You immediately contact the IT service desk to report this Personal Data Security Incident. The Data Privacy function and the Security Operations Center proceed to manage the Personal Data Security Incident in accordance with the relevant Novartis procedures.

Phishing Attack

One day an employee receives a call on her work phone. The caller claims he works for Novartis in a different country and is currently at the airport awaiting a flight to visit Novartis in another country. He requests that the employee provides him with a list of names and email address of other employees in the Novartis office so that he can schedule meetings upon his arrival. The employee wants to be helpful and promptly emails the information to the caller. After sending the information the employee realizes that she has sent the information to a non-Novartis email address, and suspect that the caller may not have been a Novartis employee after all. She promptly contacts the IT service desk to make them aware of this incident.

3.5 Principle 5 – Minimal Retention

We keep Personal Information only for as long we can legitimately use it.

3.5.1 Background

When Novartis collects Personal Information, we do so for specific purposes which we communicate to Individuals. Once we have fulfilled such purposes, we may no longer have a lawful reason to continue to hold on to the Personal Information. Unless there is a legitimate reason and legal basis to keep or use the Personal Information for secondary purposes, we should no longer keep that Information.

3.5.2 Implementation

Associates must:

- Keep Personal Information only as long as necessary for the specific purpose or as required by law. Consult your records retention schedules for specific timeframes for maintaining Personal Information.
- Ensure Personal Information collected and Processed remains necessary for the initial intended purpose and legitimate reason.
- Anonymization can be used as an alternative to deletion in some circumstances to drive further value from the data. Discuss with your local Data Privacy Business Partner if you are considering Anonymizing Personal Information.

3.5.3 Examples

Medical Information Website

The Medical team has developed an HCP restricted-access website to share scientific materials and publications related to a recent international cardiology conference. The website will be available for up to 6 months after the conference. At the conference, Novartis collects the first name, last name, email address and additional information about the HCP specialty and medical field interests. The information is collected and managed in an Excel spreadsheet.

Access to the website is given via a link sent to the HCP's email address. Since there is no other purpose anticipated than providing access to this specific website, as disclosed in the HCP Privacy Notice when we collected their Personal Information, the Medical team deletes the HCP data in the Excel spreadsheet promptly after the website is closed and no longer accessible.

Retaining Information Required by Law

Human Resources in each country or organization has implemented a procedure in order to ensure that when an associate leaves Novartis, the salary information is retained for the number of years required by the local regulation, while the remainder of the file is destroyed.

4 Implementation

4.1 Group Data Privacy Organization and How to Find your Data Privacy Business Partner

[internal link]

4.2 Reference to Group Data Privacy Intranet Site for Other Policies and Guidelines

[internal link]

4.3 Training of this Policy

Associates must familiarize themselves with this Policy and any other privacy related Novartis documents developed by either Group Data Privacy or Information Security Risk Management. Each Associate must participate in mandatory and role-based training that may be given. Training resources can be found [internal link], in addition, Associates will be invited to participate in role-specific trainings and in bi-annual e-learning courses.

4.4 Third Parties

Associates contracting Third Parties are ultimately responsible for how Third Parties conduct these activities on behalf of Novartis. The best way to ensure responsible data use by Third Parties is to strictly follow the Procurement process which includes a Third Party risk assessment, and use of appropriate contractual language.

4.5 Breach of this Policy

Failure to comply with this Policy may lead to disciplinary and other actions, up to and including termination of employment.

4.6 Local Procedures

If required due to more stringent local laws or regulations, Country organizations should implement this Policy through local functional procedures that can take the form of Standard Operating Procedures ("SOP"), guidance, procedures, or other appropriate controls. The local procedures must be reviewed periodically or ad hoc to comply with

changes in local laws, and updated as necessary. The Data Privacy Business Partner is responsible for coordinating the development and distribution of such SOPs, guidance, procedures or other controls to all Novartis divisions.

Privacy Glossary (IN ALPHABETICAL ORDER)

"Anonymization"
means the process by which Personal Information is irreversibly stripped of all identifiers and can no longer be linked back to the person. Once this is done, it is no longer considered Personal Information.

"Business Owner"
is the person who within his or her area of responsibility has been empowered by a Novartis legal entity (Data Controller) to Process Personal Information and who must ensure that Personal Information is managed in compliance with the applicable data protection requirements.

"Consent"
means any freely given, specific, revocable and informed indication of the person's agreement to the processing of his/her Personal Information.

"Database"
is a structured set of Personal Information which is arranged in a systematic or methodical way, and is accessible by electronic or other means according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

"Data Controller"
means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of Personal Information.

"Data Privacy Business Partner"
means the individual who is assigned by Group Data Privacy to guide and support the business with questions related to Data Privacy and who's contact details can be found via the Group Data Privacy Intranet site.

"Data Processor"
means the natural or legal person, which Processes Personal Information on behalf and under the instructions of the Data Controller.

"Data Subject"
means the identified or identifiable natural (and, in some jurisdictions also legal) person whose Personal Information is Processed; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity (including a social security number or a code in a clinical trial case report form in combination with other information).

"Disclosure / Disclose / Disclosed"
means making Personal Information accessible to any person or company other than the Data Subject, the Data Controller or Data Processor. This may include but is not limited to the active Transfer of Personal Information to Novartis affiliates or third parties, permitting access (including remote access), distribution or publication.

"EEA"
means the Agreement on the European Economic Area, which entered into force on 1 January 1994 and brings together the EU Member States and the three EEA EFTA

States — Iceland, Liechtenstein and Norway — in a single market, referred to as the "Internal Market".
The EEA Agreement also states that when a country becomes a member of the European Union, it shall also apply to become party to the EEA Agreement (Article 128), thus leading to an enlargement of the EEA. Switzerland is not part of the EEA Agreement, but has a bilateral agreement with the EU.

"EU"
means the European Union (EU). The EU countries are: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.

"Explicit Consent"
means that an individual is clearly presented with an option to agree or disagree with the collection, use, or disclosure of Personal Information and clearly indicates their choice.

"Individual"
means "Data Subject".

"Legitimate Business Purpose"
means a purpose which is directly or indirectly related to the business operations of Novartis and which does not interfere with the fundamental rights and freedoms of the individual. For example, HR managers may process Personal Information to perform their administrative obligation. A Legitimate Business Purpose may include compliance with legal, regulatory or ethical obligations applicable to the company.

"Master Processing Agreement (MPA)"
means an agreement signed between Novartis affiliates and Novartis Pharma AG giving general instructions to the Data Processor (Novartis Pharma AG) in order to define, in one document, rules and instructions for data Processing between Novartis companies. The MPA will also allow Novartis Pharma AG to manage interactions with Third Parties on behalf of affiliates when dealing with global projects involving global vendors and partners.

"Personal Data Security Incident"
means (a) the loss or misuse of Personal Information, (b) the accidental, unauthorized and/or unlawful access or handling of Personal Information, or (c) any other act or omission that compromises the security, confidentiality and/or integrity of Personal Information.

"Personal Information"
means all information that relates to a person where that person can be identified by you or others. In some cases, the person can be identified directly (e.g., your name or your photograph) or the person can be identified indirectly (e.g., a medical insurance number, your position in a company or by means of a study code assigned in a clinical trial).
In some countries, Personal Information may also include information such as medical device serial numbers, biological samples, IP addresses or information relating to a company ("legal person"). The definition of Personal Information may vary by country and local law should be consulted. Associates should check with their Data Privacy Business Partner for guidance.

“Privacy Notice”
means an oral or written statement that Individuals are given when Personal Information about them is being collected. The Privacy Notice describes who is collecting Personal Information, why Personal Information is being collected, how it will be used, shared, stored and any other relevant information of which the person should be aware. Oral notices may need to be recorded to establish evidence that notice was provided to the person and these requirements should be stated in local SOPs, if applicable.

“Process / Processing / Processed”
means any operation or set of operations performed upon Personal Information. This definition includes, but is not limited to, collection, recording, organization, storage, retrieval, use, disclosure, Anonymization, Pseudonymization or deletion.

“Pseudonymize”
means replacing a person’s name and most other identifying characteristics with a label, code or other artificial identifiers in order to protect against identification of the person.

“Right of Access”
means the right of the Data Subject to request and obtain from the Data Controller information regarding his/her Personal Information which is subject to Processing, at least as to the purpose of the Processing, the categories of Personal Information concerned as well as the origin of such data and its Disclosure or intended Disclosure. The Data Subject is also entitled to any other access right conferred to him/her under local applicable laws.

“Sensitive Personal Information”
is a subset of Personal Information that requires a higher level of protection. Such information may include racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, social security or insurance information, criminal charges, conviction / sentence, or a person’s sexual orientation, or health information. Data elements that make up Sensitive Personal Information may vary by country and local law should be consulted. Associates should check with their Data Privacy Business Partner for guidance. Personal Information related to health is always considered as Sensitive Personal Information at Novartis.

“Third Party”
is any person, including a legal entity, with whom Novartis interacts and that is not a Novartis company or Associate.

“Traceability”
follows the lifecycle of information to track all access and changes to Personal Information and locations of the Personal Information. It helps Novartis demonstrate transparency, compliance and adherence to regulations.

“Transfer”
means any Disclosure of Personal Information by someone other than the person to whom the Personal Information belongs. The term “Transfer” may include the physical movement of Personal Information or the provision of access to Personal Information.