Appendix 1 to Novartis BCR

Categories of Data Subjects and Processing Purposes covered by the BCR

Novartis shall process Personal Information lawfully. Lawful Processing means that Novartis will not Process Personal Information unless:

1. Novartis needs to Process the Personal Information to:
    a. perform, or take steps with a view to enter into, a contract with the relevant Data Subject;
    b. comply with a legal obligation to which Novartis is subject;
    c. protect the vital interests of the Data Subject;
2. Novartis needs to carry out such Processing to pursue Novartis' legitimate interests, and these interests do not prejudice the interests or fundamental rights and freedoms of the Data Subject concerned, in particular where Personal Information of a child is involved;
3. the Data Subject concerned has consented to the Processing, by providing a freely given, specific, informed and unambiguous indication of the Data Subject's wishes by a clear affirmative action; or
4. Applicable data protection laws otherwise permit such Processing.

Novartis shall not process Special Categories of Personal Information unless:

1. the Data Subject has given explicit consent to the processing of those Personal Information
2. Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorized by EEA+ law or a collective agreement pursuant to State law from an EEA+ country providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject;
3. Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;
4. Processing relates to Personal Information which is manifestly made public by the Data Subject;
5. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
6. Processing is necessary for reasons of substantial public interest, on the basis of EEA+ law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;
7. Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EEA+ law or pursuant to contract with a health professional;
8. Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EEA+ law which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy;

9. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with EEA+ law.

Personal Information may be Processed for a purpose other than the purpose(s) for which the Personal Information was originally collected, only if the additional purpose is compatible with the relevant original purpose, taking into account the link between the original and additional purpose, the context in which the Personal Information is collected, the nature of the relevant Personal Information and the implementation of appropriate safeguards set out below (**Secondary Purpose**).

Depending on the sensitivity of the relevant Personal Information and the possible consequences for the Data Subject, the Processing of Personal Information for the Secondary Purpose may require additional safeguarding measures (such as limiting access to the Personal Information or taking additional security measures) to mitigate the consequences. If the consequences cannot be appropriately mitigated, Novartis may need to provide the Data Subject an opt-out opportunity, or obtain the Data Subject's consent.

To the extent not already covered in this Appendix 1, and subject to the compatibility assessment, below are a number of examples of Processing for Secondary Purposes that may be permissible:

- anonymization or pseudonymization of Personal Information;
- internal audits or investigations;
- implementation of business controls and operational efficiency;
- IT systems and infrastructure related Processing such as for maintenance, support, life-cycle management, and security (including resilience and incident management);
- training of artificial intelligence systems; for the purposes of public interest, scientific or historical research purposes or statistical purposes, including the transfer of the Personal Information to an archive for these purposes;
- dispute resolution;
- legal or business consulting; or
- insurance purposes.

The Novartis BCR apply to the Processing of Personal Information, as permitted and/or required by applicable local laws, pertaining to the categories of Data Subjects listed in the table below.

The Personal Information might be retained in both physical files and electronic files for as long as it is necessary to satisfy Novartis' Legitimate Business Purposes, unless overriding legal or internal retention schedules or other legal requirements require a longer or shorter retention period.

1. EMPLOYEE PERSONAL INFORMATION

Description	Details
Categories of Data Subjects whose Personal Information is Processed	• **Present Employees**, including managers and temporary staff; • **Past Employees, job applicants, trainees, retirees**;

	• **Third party Employees**, i.e. Employees employed by third parties and working within the Novartis infrastructure, either physically on premises or virtually through the Novartis issued devices and/or Novartis accounts;
Categories of Personal Information Processed	• **General and Identification Information**, such as name, first name, last name, address, telephone, fax, e-mail, and other relevant contact details; emergency contacts; nationality; date of birth; ID card number, passport number; civil status; domestic partners'/family members'/dependents' names and dates of birth gender, photograph, and more generally, information about the activities carried out in the professional capacity, such as information included in electronic communications (e.g. emails, chat, business documents, etc.), etc.; • **Electronic identification data**, (e.g. login, access right, passwords, badge number, IP address, online identifiers/cookies, logs, access and connection times, sound or image recording such as CCTV or voice recordings); • **Social Security Information**, such as tax/social security codes/status, insurance details, sickness leave, disabilities, etc.; • **Administrative and Financial Information**, such as function; degree and job title; hire and termination date; Employee's number or code; cost center; organizational management data such as unit, department, supervisor and subordinates; credit card/bank account number, compensation details and history, such as salary, stocks, options, bonus, expense information,

	• **Talent Management Information**, such as employment and education history, other details included in the CVs; professional qualifications and experience, information necessary to complete a background check, performance and development programs and reviews and career development plans, etc.;
Special Categories of Personal Information	Special Categories of Personal Information include health and medical information and other sensitive information such as biometric data (e.g. fingerprints and iris scans), religion or church affiliation where required for statutory tax deductions; diversity-related sensitive information (such as gender, race or ethnicity) inasmuch as necessary in order to comply with legal obligations and internal policies relating to diversity and anti-discrimination; labour union membership. Other sensitive information which do not necessarily qualify as Special Category of Personal Information may be Processed: judicial data (e.g. data relating to administrative and criminal proceedings or sanctions and investigation data, identification of persons involved in proceedings, facts of a legal dispute, documentation, and nature of proceedings), insofar as necessary and legally permitted in accordance with Art. 10 GDPR, data in connection with the investigation of complaints and misconducts (including the investigation of violations of internal policies, codes and laws as well as improper behaviour), and data collected regarding harassment complaints.
Purpose(s) of Processing	• **Managing Workforce**, such as managing work activities and personnel generally, including recruitment, onboarding, training and development, performance management, appraisals, promotions and succession planning; providing the services of a data privacy officer and any related services for the management of a global privacy office; administering remuneration and other contractual benefits, salaries and

	pay reviews and other awards such as stock options, stock grants and bonuses; administering pensions and savings plans; providing benefits to Employees and their families; managing business expenses; arranging travel, relocation, transfers and secondments; making business travel arrangements; performing background checks; planning and managing professional development and skills, including training; creating and maintaining internal employee directories; managing disciplinary matters and terminations; monitoring in the workplace, IT administration (including internet, e-mails and company electronic devices monitoring) in accordance with applicable laws; performing general analytics in order to gain employment, organization and organizational culture related insights and use these insights, based on aggregated data, for improving internal processes and for benchmarking purposes; • **Communications and Emergencies**, such as facilitating communication with Employees for business purposes and for global initiatives; to be disbursed at their workplace, home and while traveling; for protecting the health and safety of Employees and others; for facilitating communication in an emergency; and for providing references; • **Maintaining Business Operations**, such as operating and managing technology and communications systems; safeguarding Company's interests and property including IT infrastructure, and office equipment; managing product and service development; improving products and services; allocating company assets and human resources; strategic planning; project management, ensuring business

	continuity, compilation of audit trails and other reporting tools; budgeting, financial management and reporting; managing mergers and acquisitions, and reorganizations or sale; • **Ensuring Compliance**, such as complying with Novartis policies and with legal requirements, such as income tax and national insurance deductions; managing and investigating alleged cases of misconduct or fraud; record-keeping and reporting obligations; conducting audits; complying with inspections and other requests from law enforcement or other public authorities; responding to legal processes such as subpoenas irrespective of whether Novartis is subject to a legal or regulatory obligation; pursuing legal rights and remedies; defending litigation and managing any internal complaints or claims, etc.; • **Conducting health risk appraisals** only as permitted and/or required by local law for the sole purpose of managing the employment relationship.

2. Consumers and Patients' Personal Information

Description	Details
Categories of Data Subjects whose Personal Information is Processed	Consumers, i.e. individuals who purchase, receive or seek information about Novartis, about Novartis' products, diseases or disease related programs dedicated to patients and their caregivers and families as well as patients who receive treatment and services for their personal use. This includes patients, prospective Consumers and healthy individuals whose data is collected through sources like: social media, applications, websites and devices. Novartis may Process the Personal Information of children for purposes of clinical trials. Where Personal Information of children is Processed, Novartis implements additional

	safeguards to protect the rights and freedoms of children;
Categories of Personal Information Processed	• **General and Identification Information**, such as name, address, telephone and fax number, e-mail address, unique identifiers, and other relevant contact details and information linked to the use of the digital channel mentioned above (i.e. conversation history, social media account information), etc.; • **Patient Support Information**, such as healthcare data and supplementary product ordering; inquiries about products and services; due diligence and other information collected in connection with consumer transactions, such as health insurance information, income, etc; online information such as user password and preferences, support queries and/or complaints, etc.;
Special Categories of Personal Information	• **Health Information**, such as physical characteristics (weight, height, blood type, etc.); genetic data, biological samples, prescription information and disease-related information, lifestyle information (smoking habits, alcohol use, etc.), dietary preferences, general health information, information collected through patient support programs, etc.;
Purpose(s) of the Processing	• **Patient and consumers support** Information, patient programs and research, such as providing healthcare and other services; meeting specific requests from consumers regarding products and services; technical and other support; developing and manufacturing new drugs from patients' cells or any other biological component in the context of personalized medicine; managing product and service development and delivery; managing focus groups; managing disease awareness programs; managing patient support programs; conducting

	market and development research for new products; marketing and sales of products and services; spontaneous adverse event reporting concerning drug safety or product complaint; facilitating communication with customers including marketing communications and other general marketing activities such as consumer testimonials and feedback concerning services and products, etc.; supporting future scientific research purposes advancing science and public health; • **Ensuring Compliance**, such as complying with Novartis policies and with legal requirements, such as income tax and national insurance deductions; record-keeping and reporting obligations; conducting audits; managing mergers and acquisitions, and reorganizations or sale; detecting fraud; complying with inspections and other requests from law enforcement or other public authorities; responding to legal processes such as subpoenas irrespective of whether Novartis is subject to a legal or regulatory obligation; pursuing legal rights and remedies; defending litigation and managing any internal complaints or claims, etc.

3. Business customers' Personal Information

Description	Details
Categories of Data Subjects whose Personal Information is Transferred	• Where **legal persons** are covered by local data protection laws: legal entities such as hospitals, Clinical Research Organizations (CRO), managed care organizations, insurance providers and other healthcare providers, governmental agencies and other public authorities, retail outlets and any other legal entity that provides healthcare products and services to the public;

	• **Individuals acting on behalf of the legal entities mentioned above**; • **Healthcare Professionals** including physicians, nurses, pharmacists, veterinarians, etc.
Categories of Personal Information Transferred	• **General and Identification Information**, such as name; address, telephone and fax number, e-mail address, company or healthcare institution; and other relevant contact details; • **Professional Background**, such as details contained in CVs; educational and professional background; professional career achievements including specialization, academic and professional degrees and titles, licenses; publications; memberships in professional associations; and other information concerning preferences, , professional background and development; • **Financial & Transactional Information**, such as information collected for the purpose of establishing and maintaining relationships with Novartis; information collected in connection with sales and promotional activities, including profiling and future potential interactions; financial information including transaction details, bank details, payment methods and terms; travel information, information regarding utilization, responses and/or preferences including in terms of types of messages discussed, channels of communication and frequency;
Special Categories of Personal Information	[N/A]
Purpose(s) of the Transfer and further Processing	• **Sales and Marketing**, such as providing Business Customers and Other Stakeholders with appropriate, adequate and updated information about disease, drugs as well as Novartis products and services, improving the quality of our interactions and services, managing communications and interactions with Business Customers, tracking Novartis

	activities (e.g. measuring interactions and number of appointments/calls), enlisting specialists for speaking engagements and congresses, soliciting expert advice regarding new products and services, etc.; • **Business Operations**, such as managing product and service delivery; contract management and related financial transactions including invoicing for services and any transparency obligations; travel and expense management; and spontaneous adverse event and quality reporting concerning drug safety or product complaints; • **Ensuring Compliance**, such as complying with Novartis policies and with legal requirements, such as income tax and national insurance deductions; record-keeping and reporting obligations; conducting audits; managing mergers and acquisitions, and reorganizations or sale; complying with inspections and other requests from law enforcement or other public authorities; responding to legal process such as subpoenas irrespective of whether Novartis is subject to a legal or regulatory obligation; pursuing legal rights and remedies; defending litigation and managing any internal complains or claims, etc.

4. Vendors and Business partners' Personal Information

Description	Details
Categories of Data Subjects whose Personal Information is Transferred	• **Legal entities of vendors and business partners** in countries that protect legal persons under their local data protection laws; • **Individuals acting on behalf of legal entities mentioned above;** • **Consultants, independent contractors, and agents**.

Categories of Personal Information Transferred	• **General and Identification Information**, such as name, address, telephone, fax, e-mail, and other contact details; • **Financial and Transactional Information**, such as information collected in connection with vendor and business partner transactions, financial information including tax number, classification, bank details, payment methods and terms, and due diligence information on Vendors and Business Partners.
Special Categories of Personal Information Transferred	[N/A]
Purpose(s) of the Transfer and further Processing	• **Financial & Transactional**, such as establishing and maintaining business relationships with the respective Vendors and or Business Partners and managing contractual and financial obligations; • **Business Operations**, such as managing product and service development, including product joint ventures, joint publications, strategic planning, project management, financial management and reporting, business development and licensing; • **Ensuring Compliance**, such as complying with Novartis policies and with legal requirements, including income tax and national insurance deductions; record-keeping and reporting obligations; conducting audits; managing mergers and acquisitions, and reorganizations or sale; complying with inspections and other requests from law enforcement or other public authorities; responding to legal processes such as subpoenas irrespective of whether Novartis is subject to a legal or regulatory obligation; pursuing legal rights and remedies; defending litigation and managing any internal complaints or claims.

5. Research and Pharmacovigilance Personal Information

Description	Details
Categories of Data Subjects whose Personal Information is Processed	• **Research Participants**, including Patients who are individuals affected with a disease or condition and healthy volunteers enrolled in the early phase of clinical trials; • **Healthcare Professionals** who conduct biomedical or other research on behalf of Novartis, including physicians, pharmacists, nurses, and the supporting technical and research staff, etc.,

Categories of Personal Information Processed	• **General and Identification Information**, concerning:
	  ○ Research Participants, such as clinical trial codes, initials, date of birth, gender, Research Participant's name and contact information when collected for adverse event reporting;
	  ○ Healthcare Professionals, such as name, address, telephone, fax, e-mail, and other contact details;
	
	• **Financial and Transactional Information**, concerning Healthcare Professionals such as information collected for the purpose of establishing and maintaining relationships with Novartis; information collected in connection with the conduct of a clinical trial; financial information including transaction details, bank details, payment method and terms; travel information and profile;
	
	• **Professional Background** concerning Healthcare Professionals, such as details contained in CVs; educational and professional background; professional career achievements including specialization, academic and professional degrees and titles, licenses; publications; memberships in professional associations; and other information concerning professional background and development;

Special Categories of Personal Information	• **Health Information** concerning Research Participants, such as physical characteristics, medical history, including medical history in the family, biological tissue samples (blood, sputum, urine, etc.), including extracted genetic data (DNA/RNA), lifestyle information (fitness and physical exercise, smoking habits, alcohol use, etc.), accelerometry or motion detection data, dietary preferences, event onset and end dates, vital signs, biomarkers, dose administration, adverse events, protocol specific measures (labs, images, MRs, x-rays, diary), lab data, concomitant drugs, etc.; • **Other Special Categories of Personal Information** concerning Research Participants, such as race or ethnic origin, sex life, etc.
Purpose(s) of the Processing	• **Business Operations**, such as conducting and managing preclinical, clinical and biological research, genomic and genetic research, developing new drugs, managing biological samples, managing clinical trial systems and non-interventional studies, supporting future scientific research purposes advancing science and public health • **Administering Pharmacovigilance Activities**, such as complying with regulatory reporting obligations, reporting and managing adverse events and effects that occurred during the biomedical and clinical research and after the products have been approved for use, analyzing of drug safety data for triggers and trends; • **Financial and Contractual Obligations** concerning Healthcare Professionals, such as contract management and related financial transactions including invoicing for services; travel and expense management; • **Ensuring Compliance**, such as complying with Novartis policies and with legal requirements, including income tax and national insurance deductions; record-keeping and regulatory

	reporting obligations; conducting audits; managing mergers and acquisitions, and reorganizations or sale; quality management; complying with inspections and other requests from law enforcement or other public authorities; responding to legal process such as subpoenas irrespective of whether Novartis is subject to a legal or regulatory obligation; pursuing legal rights and remedies; defending litigation and managing any internal complaints or claims, etc.

Version History

Effective Date	Owner	Version	CNIL
3 July 2012	Group Data Privacy	1.0	3 July 2012
3 September 2018	Group Data Privacy	2.0	3 September 2018
20 December 2024	Head Data Privacy Digital & AI Compliance Region Europe	3.0	20 December 2024