

Appendix 6 to Novartis BCR

Privacy Organization at Novartis

1. GLOBAL DIGITAL, DATA PRIVACY & AI COMPLIANCE ORGANIZATION

Novartis has established a Data Privacy Program to ensure compliance with data protection laws, manage Data Privacy risk, enable new business models, strengthen capabilities and operate effectively and efficiently.

The Data Privacy Program is structured around the following pillars:

- the **Global Data Privacy, Digital & AI Compliance (DPDAI) Organization** under Novartis Ethics, Risk & Compliance:
- the **Novartis Data Privacy and AI policy framework and processes**, including the Novartis BCR:
- the **Data Privacy Central Monitoring program**.

The Global DPDAI Organization consists of the **Global Head DPDAI**, the **Director DPDAI Innovation, Strategy & Engagement**, the **Corporate DPDAI Team**, as well as three **regional DPDAI Teams** corresponding to the main business geographies, i.e. Americas, Europe, and Asia Pacific, Middle East & Africa (APMA). It is complemented by the **DPDAI Monitoring & reporting Team**, established under the Corporate Ethics, Risk & Compliance Organization, and by the **Data Privacy Legal Advisory Team**, established under the Legal organization.

The Global DPDAI Organization is led by the **DPDAI Leadership Team (DPDAI LT)**, which is chaired by the **Global Head DPDAI**. The DPDAI LT includes the **Head of Corporate DPDAI**, the **Head DPDAI Americas**, the **Head DPDAI Region Europe**, the **Head DPDAI APMA**, and the **Head Data Privacy Legal Advisory**. The extended DPDAI LT includes also the Head DPDAI Germany, the Head DPDAI China, the Head DPDAI Japan, the Head DPDAI Latin America & Canada, and the Head DPDAI Monitoring & Reporting. The DPDAI LT establishes and implements strategic directions for Data Privacy, sets priorities and supervises the implementation of effective controls.

The **Global Head DPDAI** informs and advises the highest level of Novartis management, monitors, and annually reports on, compliance with Data Privacy laws and regulations at a global level, and oversees the maintenance and adherence to the Group Privacy Program. He/she reports to the Novartis Chief Ethics, Risk & Compliance Officer, who is a member of the Executive Committee of Novartis (ECN).

Novartis retains an external Data Privacy expert to serve as **Group Data Protection Officer (GDPO)** for the Novartis legal entities established in European Economic Area and the United Kingdom, and a Data Protection Officer for Switzerland. The GDPO is independent and receives regular updates from the DPDAI LT on the status of the implementation of the Novartis Data Privacy program. The GDPO supports the Global Head DPDAI in fulfilling their core responsibilities as described above. The GDPO should not have any tasks that could result in conflict of interests.

The **Director Innovation, Strategy & Engagement, DPDAI**, by closely engaging business stakeholders, evaluates their perceptions and increases their awareness of the DPDAI function, with the objective to maximize the impact of it, and to generate recommendations to the DPDAI teams on how to implement appropriate and impactful initiatives. She/he also

manages all DPDAI-related global communications and awareness/training initiatives within the DPDAI function, Novartis Ethics, Risk & Compliance and Novartis as a whole.

The **Head Corporate DPDAI** defines group wide compliance standards, supports global business stakeholders and functions to identify privacy risk and implement privacy controls across Novartis, provides risk assurance to Novartis management, designs key global data privacy processes to document and demonstrate compliance with all relevant data privacy laws and regulations worldwide, leads the management and resolution of data privacy incidents.

The **Heads DPDAI Americas, Region Europe and APMA**, within the geographies they are responsible for, ensure adequate staffing and provide leadership, support and coaching to the country DPDAI Heads. They are responsible for ensuring strong business partnership on Data Privacy matters and operational efficiency within their region of responsibility.

In addition to the major EEA+ markets (Germany, France, Spain, Italy, United Kingdom), many countries in EEA+ and in the other regions have appointed full time **Country DPDAI Heads** and/or **Data Privacy Managers** responsible for overseeing the implementation of the Novartis Data Privacy program within the countries of their responsibility, providing business partnering support and competent advice on Data Privacy matters, handling of local requests and complaints from Data Subjects, reporting major privacy issues to the Head DPDAI responsible for their respective Regions, and ensuring training and awareness of Data Privacy at a local level. **Country DPDAI Heads** report operationally to the DPDAI Head of the relevant region. The **Head Data Privacy Legal Advisory (DPLA)** ensures the provision of legal advice to DPDAI on higher risk Privacy matters by leading the DPLA Team. DPLA, established under the Legal function, is responsible for monitoring legislations and regulatory developments in Privacy, Cybersecurity and AI across the globe to identify new requirements and potential implementation steps. DPLA is also handling legal aspects of personal data incidents and forming part of the Legal incident response team to Cybersecurity incidents.

The **Head DPDAI Monitoring and Reporting** is responsible for regularly monitoring the implementation of the Novartis Data Privacy program within the different Novartis organizational units. This is done to ensure compliance with applicable laws, regulations, and relevant Novartis policies, handbooks, and guidance documents. She/he also regularly provides reports and insights to the Global Head DPDAI on major and emerging risks and trends. The Head DPDAI Monitoring and Reporting reports into the Head Review, Monitoring & Remediation under Corporate Ethics, Risk & Compliance.

The **Assistant to the Global Head DPDAI** supports the DPDAI LT and manages associated administrative tasks and is responsible for providing professional support to the Global Head DPDAI, executing complex administrative tasks, and managing the operational budget of the department.

2. NOVARTIS CHIEF ETHICS, RISK & COMPLIANCE OFFICER

The **Novartis** Chief Ethics, Risk & Compliance Officer (**CERCO**), a member of the Novartis Executive Committee, supervises the Global Head Data Privacy and Group Data Protection Officer. The CERCO receives regular updates on the status of the Privacy Program.

3. COMMUNICATION AND COORDINATION

The communication, coordination and collaboration within the Global DPDAI Organization is driven by the Director Innovation, Strategy & Engagement supported by the DPDAI Intranet site that contains privacy vision and strategic priorities, contact details of the relevant DPDAI business partners, guidelines, templates, tools and meaningful updates.

Version History for Annex 6

Effective Date	Owner	Version	CNIL
3 July 2012	Group Data Privacy	1.0	3 July 2012
19 April 2017	Group Data Privacy	2.0	19 April 2017
3 September 2018	Group Data Privacy	3.0	3 September 2018
5 September 2019	Group Data Privacy	4.0	5 September 2019
20 December 2024	Head Data Privacy Digital & AI Compliance Region Europe	5.0	20 December 2024