Data Protection Regulations of the Novartis Pension Funds

Objectives

These regulations specify the privacy policy of the Novartis Pension Funds[1]. The principles set forth therein serve to protect natural persons and legal entities from any misuse of personal data processed by the pension funds within the scope of their legal, statutory and regulatory mandate.

It regulates the handling of personal data that is obtained, used, disclosed, modified, stored, archived or destroyed within the scope of and in connection with the management of the business, including any service, support and management processes of the Novartis Pension Funds.

As pension provider of a renowned founder company, the Novartis Pension Funds treat the protection of personal data of their insured members with particular care. The *Data Privacy Policy* and the relevant *Key Directives, Guidelines & Instructions of* the founder company are also binding and directly applicable for the Novartis Pension Funds[2].

There is an annual compliance and risk assessment[3] .

Core elements of data protection:

- Admissibility and purpose
- Proportionality ("data economy")
- Information and consent of the persons concerned
- Transparency
- Data quality and timeliness
- Retention periods
- Information Security
- Data protection "awareness
- Disclosure to third parties
- Cross-border data transfer

1. Admissibility and purpose

The collection, storage and use of personal data, i.e., of any information relating to an identified or identifiable person, is permitted from finally in accordance with the legal, statutory and regulatory provisions and only for the declared purpose, i.e., for the implementation of the occupational pension plan.

---

[1] In order to advise the employees of the founder company professionally, independently and with the highest level of expertise in all pension and insurance matters, the Novartis Pension Funds are affiliated with the organizational unit *Insurance Consulting Novartis,* which specializes in insurance matters. For reasons of clarity and due to the special requirements of its business area, this unit has its own data protection regulations.

[2] GPOL-8107309 (novartis.net)

[3] S. Annex 1 to these regulations

2. Personal data ("data economy")

The Novartis Pension Funds only collect data that are required for the fulfillment of their legal, statutory and regulatory tasks. This data is generally included in the insurance certificate and thus also complies with the relevant information requirements of the BVG:

- Name, first name
- Date of birth, date of death
- Gender
- Marital status
- Addresses
- E-mail / Phone number
- Personnel number (identification feature for the personnel data system)
- Languages
- Wage company
- AHV number
- Social security number
- Employee category
- Entry to company and cash register
- Employment level
- Total relevant income
- Assets/capital
- Incentive/Bonus
- Shift bonus
- Marriage/divorce date
- Advance withdrawal/pledge data (WEF/divorce)
- Purchasing services
- Move-in date
- Vested benefits
- Defined retirement and risk benefits
- Contribution data
- Beneficiary agreements

As a matter of principle, data and information that qualify as particularly worthy of protection are not collected, namely:

- Religious, ideological, or political beliefs
- Trade union activity
- Race and ethnic origin
- Privacy
- Criminal proceedings or sanctions.

Health data (namely health declarations, medical reports, access to files of the IV and other social insurance institutions, etc.) must be collected, used, and stored with special care within the framework of the execution of the legal, statutory and regulatory tasks.

3. Information and consent of the people concerned

The data collection must be recognizable for the data subject; if necessary, his or her consent must be obtained.

4. Transparency - rights of data subjects

Any data subject has the right to request access to data and the correction of inaccurate or incomplete data. The right includes:

- The right to be informed about what personal data we hold about you and how we process your personal data;
- The right to access the personal data we process and, if you believe that the data concerning you is inaccurate, out of date or incomplete, to request that it be corrected or updated;
- the right to request the erasure of your personal data or its restriction to certain categories of processing;
- the right to withdraw your consent at any time without affecting the lawfulness of the processing prior to this withdrawal;
- the right to object, in whole or in part, to the processing of your personal data. With certain exceptions, this includes the right to object to direct marketing and the right to object to the use of your personal data for research purposes;
- The right to request data portability, which means that the personal data you have provided to us will be returned to you or transferred to a person of your choice, in a structured, commonly used and machine-readable format, without our preventing you from doing so and subject to your confidentiality obligations; and
- the right to object to automated decision-making, including profiling, which produces significant effects or legal effects, i.e., you may request that a human being intervene in an automated decision-making process involving processing of your data which produces significant effects or legal effects and where such processing is not based on your consent, is lawful or necessary for the performance of a contract. However, we do not currently make decisions based solely on automated processes that have significant or legal effects on individuals.

Corresponding requests should be sent to: Novartis Pension Funds, P.O. Box, 4002 Basel or by e-mail to: pk.privacy@novartis.com.

5. Data quality and up-to-datedness

The Novartis Pension Funds take appropriate quality assurance measures to ensure the accuracy of the personal data processed.

- A data interface must be maintained with the respective systems of the founder company, which ensures that the pension fund data is always up to date and, conversely, that the founder company always has access to the latest pension fund-specific data (contributions, benefits). In addition, the data can be updated by the insured person at any time.
- The data processing is carried out by authorized personnel only.

6. Storage

Personal data will generally only be retained for as long as is necessary to fulfill the purpose for which it was collected or to comply with legal or regulatory requirements. If pension benefits are paid out, the obligation to keep records lasts until ten years after the end of the obligation to pay benefits. If no pension benefits are paid out because the insured person has not claimed them, there is a duty to retain the records until the insured person reaches or would have reached the age of 100.

7. Protection against unauthorized access and destruction (information security)[4]

7.1 Access control

- The premises of the Novartis Pension Funds are particularly secured.
- Electronic data may only be stored on servers of the founder company in secured data centers that are not accessible to the public and have a secured access system.
- These data centers are only accessible to authorized employees.

7.2 Right to use control

- The granting of access rights to personal data and the IT management system of the Novartis Pension Funds must be handled restrictively. The authority for this lies with the Managing Director.
- Unused accounts are to be deleted.
- On the premises of the Novartis Pension Funds, it must be ensured that no unauthorized access to data is possible for visitors.
- The founder company's guidelines on password security apply.
- In accordance with the relevant IT standards of the founder company, access passwords shall be changed on the prescribed cycle.

[4] For information security, see also Appendix 2 to these regulations.

7.3 User control

- Access to the data stored electronically as well as in paper form is reserved for authorized employees of the office.

7.4 Transfer control[5]

- Data transmitted via interfaces to the foundation company may only be sent to the offices authorized for this purpose within the scope of their intended task (contribution invoicing, pension payments).
- Classified data carriers must be marked as such (e.g., "confidential" or "personal"). They must be packaged and addressed accordingly.
- The guidelines issued by the founder company for the secure use of fax, Internet, etc. apply. Mail with confidential data is to be sent via "Secure Novartis Mail System".

7.5 Input control

- Data processing is carried out by authorized employees of the office either via the interface or manually. The entries are logged (logbook)**.**

7.6 Outsourcing control:

- If the processing of personal data is outsourced to third parties, these must be contractually obligated to comply with the data protection requirements of the client, e.g., by means of special agreements in the relevant service level agreements.
- The Novartis Pension Funds, as the contracting party, reserve the corresponding control powers and duly exercise them, for example by inspecting the relevant regulations and internal directives of the third party.

7.7 Availability control

- In the event of a pandemic or other use cases as part of the pension funds' Emergency & Business Continuity planning, the access codes are stored in the pension funds' own safe and are specially secured.
- Server rooms are protected against external influences.
- Backup (automatic and daily) and data readback must be tested regularly.
- The server content is backed up using a virtual backup server, whereby the virtual ser ver must not be located in the same data center.
- The data must be backed up in such a way that it can be reproduced within a reasonable period of time even in the event of a disaster (loss, destruction or damage) (daily data mirroring).

[5] For information on the transfer of data to third parties, see. Section 9 f. of these regulations

7.8 Separation control

- The data collected may only be used for the purpose of managing the occupational pension plans of the Novartis Pension Funds.
- The disaster and test system has its own database.

7.9 Further controls and instructions

- A clear desk policy applies.
- The screen must be secured when leaving the office for a short time (password-protected)
- The hard disk of the notebook is encrypted.

8. Data protection "awareness"

Regular training for employees of the Novartis Pension Funds is intended to create an understanding of data protection issues, raise awareness of problems, and ensure compliance with the requirements in this regard. Participation in the interactive awareness tests offered by the founder company is mandatory. Attendance at external continuing education courses is supported.

9. Disclosure of data to third parties

- Personal data may only be disclosed to third parties within the legal framework (Article 86a BVG, if applicable in conjunction with the general administrative assistance provision pursuant to Article 32 ATSG) or on the basis of the express written consent of the person concerned. The life partner or spouse of the insured person is also deemed to be a third party. Consents or powers of attorney granted in writing are valid until revoked.
- Contractors of the Novartis Pension Funds who have a special mandate relationship with the pension funds as provided for by law, such as Experts for occupational benefits, Auditors or reinsurers, are in principle subject to the same duty of confidentiality and data protection as the commissioning pension fund. Nevertheless, the personal data disclosed within the scope of and for the fulfillment of the corresponding mandates must be anonymized as far as possible.
- The consent of the person concerned is required for the disclosure of data to internal departments of the founding company (e.g., *People & Organization, Rewards).* If consent cannot be obtained in urgent cases, data may nevertheless be disclosed, if necessary and by way of exception, provided that it can be assumed that disclosure is in the well-understood interest of the insured person (e.g. for internal transfer calculations within the Group, in connection with the search for optimized pension solutions in the event of termination of the employment contract, early retirement, external insurance options, etc.).
- It is also permitted to pass on specific insured person data if this is required by the founder company in order for it to be able to fulfill certain statutory information obligations (e.g., SWX, Annual Report, Annual Report, and similar public reports).

- Data required by the founding company for the preparation of documentation and overview brochures for the data subject himself/herself (Total Compensation Report) may be disclosed if the consent of the data subject can be conclusively demonstrated.

10. Cross-border data transfer

In principle, the data will be forwarded to the data subject, unless the data subject expressly authorizes a direct transfer. The corresponding guidelines of the founding company on the cross-border exchange of data must be applied.

For transfers of personal data between Novartis subsidiaries and affiliates, Novartis has implemented the Binding Corporate Rules. This is a system of principles, rules and instruments authorized by European law to govern the transfer of personal data outside the EEA and Switzerland. Click here to learn more about the Novartis Corporate Rules.

11. Miscellaneous

11.1 Internal audit

The data protection officer of the Novartis Pension Funds is called in to conduct periodic internal audits. The audit points are jointly defined on the basis of a comprehensive checklist, and the audit results are recorded.

11.2 Homepage of the Novartis Pension Funds

The Novartis pension funds have their own electronic website.

http://www.pensionskassen-novartis.ch

This is for general information purposes only and does not contain any information that allows conclusions to be drawn about individual insured persons.