Data Protection Regulations Insurance Services Novartis

Destination

The present regulations substantiate the data protection declaration of Insurance Services Novartis[1]. The principles set forth therein serve to protect natural persons and legal entities from any misuse of personal data processed by Insurance Services Novartis within the scope of its service mandate.

It bindingly regulates the handling of personal data that is procured, used, disclosed, modified, stored, archived or destroyed within the scope of and in connection with the the business of Insurance Services Novartis. This business includes all service, support and management processes.

Insurance Services Novartis shall treat the protection of personal data of its consulting clients with special care and in accordance with the relevant special legal requirements (namely the KVG). In addition, the Data Privacy Policy and the relevant Key Directives, Guidelines & Instructions of Novartis are also binding and directly applicable to Insurance Services Novartis[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 ultimately permitted from in accordance with the provisions of the performance mandate and only for the stated purpose.

---

[1] *Insurance Services Novartis* is affiliated with the *Novartis Pension Funds* as a specialized organizational unit in order to provide professional, independent and highly competent advice from a single source to the employees of the founding company in all pension and insurance matters. For reasons of clarity and due to the special requirements of its business area, Insurance Services Novartis has its own data protection regulations.

[2] GPOL-8107309 (novartis.net)

[3] S. Annex 1 to these regulations

2. Personal data ("data economy")

Only data that is required for the fulfillment of the purpose on the basis of the legal tasks and within the scope of the performance mandate will be collected. Personal data is only recorded to the extent that it is required to prepare an offer:

- Name, first name
- Date of birth
- Address
- Marital status
- Nationality
- Personnel number (identification feature for the personnel data system)
- Wage company
- Gender
- Language
- Start of residency

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 questionnaires on the state of health) are collected solely within the framework of the mandate, in particular in connection with specifically requested insurance supplements, and are forwarded to the corresponding insurance companies with particular care.

3. Information and consent of the persons concerned

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

4. Transparency - rights of data subjects

Any person concerned has the right to request access to his or her 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.

Pertinent requests should be sent to: Novartis Pension Funds, Aeschenvorstadt 55, P.O. Box, 4002 Basel or by e-mail to: pk.novartis@novartis.com.

5. Data quality and up-to-dateness

Insurance Services Novartis takes appropriate quality assurance measures to ensure the accuracy of the personal data processed.

- Data must be exchanged with the respective providers to ensure that this data is always up to date (e.g., invoicing in the health insurance sector).
- Data processing is performed by authorized employees of Insurance Services Novartis.

6. Storage

Personal data will generally be retained only as long as necessary to fulfill the purpose for which it was collected or to comply with legal or regulatory requirements. Insurance Services Novartis records the application data and forwards it to the relevant insurers. Data that is no longer required will be destroyed immediately.

Paper documents are to be destroyed in such a way that they cannot be reconstructed. If necessary, the documents are to be collected by specialized providers in locked containers and disposed of in a supervised manner.

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

7.1 Access control

- The premises of Insurance Services Novartis are specially secured.
- Electronic data may only be stored on Novartis servers in secure, non-publicly accessible data centers with a secured access system.
- These data centers are accessible only to authorized employees.

7.2 Right to use control

- The granting of access rights to personal data and IT systems must be handled restrictively. The authority for this lies with the CEO of the Novartis Pension Fund.
- Unused accounts are to be deleted.
- On the premises of Insurance Services Novartis, it must be ensured that no unauthorized access to data is possible for visitors, either on the screen or on paper files.
- Novartis password security guidelines apply.
- In accordance with the relevant Novartis IT standards, access passwords shall be changed on the prescribed cycle.

7.3 User control

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

7.4 Transfer control[5]

- Data transmitted via interfaces or by other means may only be delivered in a secure manner to the offices authorized for this purpose within the scope of their intended task. A record must be kept of the transfer.
- The same applies to the exchange of data with third parties in a contractual relationship.
- Classified data carriers must be marked as such (e.g. "confidential" or "personal"). They must be packaged and addressed accordingly.
- The Novartis guidelines for the secure use of fax, internet etc. apply.) Mail with confidential data must be sent via "Secure Novartis Mail system".

7.5 Input control

- Data processing is carried out by authorized employees of the insurance consultancy either via the interface or manually.

[4] For information security, see also Appendix 2 to these regulations.
[5] For information on the transfer of data to third parties, see. Section 9 f. of these regulations

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.
- As the client, Novartis Insurance Services reserves the corresponding control powers and duly exercises them, for example by inspecting the relevant regulations and internal directives of the third party.

7.7 Availability control

- 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 server 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).

7.8 Separation control

- Data may only be collected within the scope of the service mandate of Novartis Insurance Services.
- There is no access to the data collection of the Novartis pension fund.

7.9 Further controls and instructions

- Data requiring special protection is locked in appropriate file cabinets when leaving the office.
- A clear desk policy applies when leaving the office.
- 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 Novartis Insurance Services 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 Novartis is mandatory. Attendance at external training courses is supported.

9. Disclosure of data to third parties

- Personal data may only be disclosed to third parties within the scope of the performance mandate or on the basis of the express written consent of the person concerned. The life partner or spouse of the person concerned is also deemed to be a third party. Consents or powers of attorney granted in writing are valid until revoked.
- Contractors of Insurance Services Novartis who have a special mandate relationship with it as provided for by law, e.g. the Control Authority, are in principle subject to the same duty of confidentiality and data protection as the Principal. Nevertheless, the personal data disclosed within the scope of and for the fulfillment of the corresponding mandates shall be anonymized as far as possible.
- The consent of the data subject is required for the disclosure of data to internal departments of Novartis (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.

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 relevant Novartis guidelines 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 Binding Corporate Rules.

11. Miscellaneous

11.1 Internal audit

The data protection officer of the Novartis Pension Fund 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 Insurance Services homepage

The insurance consultancy has its own electronic website.

http://www.versicherungsberatung-novartis.ch

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