Datenschutzreglement Versicherungsberatung Novartis

Ziel

Das vorliegende Reglement konkretisiert die Datenschutzerklärung der Versicherungsberatung Novartis[1]. Die darin festgehaltenen Grundsätze dienen dem Schutz von natürlichen und juristischen Personen vor einem allfälligen Missbrauch von Personendaten, die durch die Versicherungsberatung Novartis im Rahmen ihres Leistungsauftrags bearbeitet werden.

Es regelt verbindlich den Umgang mit Personendaten, welche im Rahmen und aus Anlass der Besorgung der Geschäfte der Versicherungsberatung Novartis beschafft, verwendet, bekannt gegeben, verändert, aufbewahrt, archiviert oder vernichtet werden. Diese Geschäfte umfassen sämtliche Dienstleistungs-, Support- und Führungsprozesse der Versicherungsberatung Novartis.

Die Versicherungsberatung Novartis behandelt den Schutz von Personendaten ihrer Beratungskunden mit besonderer Sorgfalt und im Einklang mit den einschlägigen spezialgesetzlichen Anforderungen (namentlich des KVG). Im Übrigen sind *die* Data Privacy Policy sowie die einschlägigen Key-Directives, Guidelines & Instructions von Novartis auch für die Versicherungsberatung verbindlich und direkt anwendbar[2].

Es findet eine jährliche Konformitäts- und Risikoprüfung statt[3].

Kernelemente des Datenschutzes:

- Zulässigkeit und Zweckbestimmung
- Verhältnismässigkeit („Datensparsamkeit“)
- Information und Einverständnis der Betroffenen
- Transparenz
- Datenqualität und -aktualität
- Aufbewahrungsfristen
- Informationssicherheit
- Datenschutz-„Awareness“
- Weitergabe an Dritte
- Grenzüberschreitender Datentransfer

1. Zulässigkeit und Zweckbestimmung

Die Erhebung, Speicherung und Verwendung von Personendaten, d.h. von jeglichen Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen, ist ausschliesslich im Einklang mit den Bestimmungen des Leistungsauftrags und nur für den erklärten Zweck zulässig.

---

[1] Die *Versicherungsberatung Novartis* ist als spezialisierte Organisationseinheit den *Pensionskassen Novartis* angegliedert, um die Mitarbeitenden der Stifterfirma in allen Vorsorge- und Versicherungsbelangen professionell, unabhängig und mit höchster fachlicher Kompetenz aus einer Hand zu beraten. Aus Gründen der Übersichtlichkeit und aufgrund der besonderen Anforderungen ihres Geschäftsbereichs verfügt die Versicherungsberatung Novartis über ein eigenes Datenschutzreglement.

[2] GPOL-8107309 (novartis.net)

[3] S. Anhang 1 zu diesem Reglement

2. Personendaten („Datensparsamkeit“)

Es werden nur Daten erhoben, die zur Zweckerfüllung auf der Grundlage der gesetzlichen Aufgaben und im Rahmen des Leistungsauftrags erforderlich sind. Personendaten werden nur soweit aufgenommen, als sie zur Erstellung einer Offerte benötigt werden:

- Name, Vorname
- Geburtsdatum
- Adresse
- Zivilstand
- Nationalität
- Personalnummer (Identifikations- Merkmal zum Personaldatensystem)
- Lohnfirma
- Geschlecht
- Sprache
- Beginn Wohnsitznahme

Prinzipiell nicht erhoben werden Daten und Angaben, die als besonders schützenswert zu qualifizieren sind, namentlich:

- Religiöse, weltanschauliche oder politische Überzeugungen
- Gewerkschaftliche Tätigkeit
- Rassenzugehörigkeit und ethnische Herkunft
- Intimsphäre
- Strafrechtliche Verfahren oder Sanktionen

Gesundheitsdaten (namentlich Fragebogen zum Gesundheitszustand) sind ausschliesslich im Rahmen des Leistungsauftrags, insbesondere im Zusammenhang mit speziell gewünschten Versicherungszusätzen nach VVG zu erheben und werden mit besonderer Sorgfalt an die entsprechenden Versicherungsgesellschaften weitergeleitet.

3. Information und Einverständnis der Betroffenen

Die Datenbeschaffung muss für die betroffene Person erkennbar sein; gegebenenfalls ist ihr Einverständnis einzuholen.

4. Transparenz - Rechte der betroffenen Personen

Jede betroffene Person hat das Recht, Dateneinsicht sowie die Korrektur unzutreffender oder unvollständiger Daten zu verlangen. Der Anspruch umfasst:

- das Recht, darüber informiert zu werden, welche persönlichen Daten wir über Sie haben und wie wir Ihre persönlichen Daten verarbeiten;
- das Recht, auf die von uns verarbeiteten personenbezogenen Daten zuzugreifen und, wenn Sie der Meinung sind, dass die Sie betreffenden Daten unrichtig, veraltet oder unvollständig sind, deren Berichtigung oder Aktualisierung zu verlangen;

- das Recht, die Löschung Ihrer personenbezogenen Daten oder deren Einschränkung auf bestimmte Kategorien der Verarbeitung zu verlangen;
- das Recht, Ihre Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmässigkeit der Verarbeitung vor diesem Widerruf berührt wird;
- das Recht, der Verarbeitung Ihrer personenbezogenen Daten ganz oder teilweise zu widersprechen. Mit bestimmten Ausnahmen umfasst dies das Recht, der Direktwerbung zu widersprechen und das Recht, der Verwendung Ihrer personenbezogenen Daten zu Forschungszwecken zu widersprechen;
- das Recht, eine Datenübertragbarkeit zu beantragen, d.h. dass die personenbezogenen Daten, die Sie uns zur Verfügung gestellt haben, an Sie zurückgegeben oder an eine Person Ihrer Wahl übertragen werden, und zwar in einem strukturierten, allgemein verwendeten und maschinenlesbaren Format, ohne dass wir Sie daran hindern, und vorbehaltlich Ihrer Vertraulichkeitsverpflichtungen; und
- das Recht, einer automatisierten Entscheidungsfindung einschliesslich Profiling zu widersprechen, die erhebliche oder rechtliche Auswirkungen hat, d. h. Sie können verlangen, dass ein Mensch in einen automatisierten Entscheidungsfindungsprozess eingreift, der mit einer Verarbeitung Ihrer Daten verbunden ist, die erhebliche oder rechtliche Auswirkungen hat, und wenn eine solche Verarbeitung nicht auf Ihrer Einwilligung beruht, gesetzlich zulässig oder für die Erfüllung eines Vertrags erforderlich ist. Allerdings treffen wir derzeit keine Entscheidungen, die ausschliesslich auf automatisierten Verfahren beruhen und erhebliche oder rechtliche Auswirkungen auf den Einzelnen haben.

Entsprechende Begehren sind zu richten an: Pensionskassen Novartis, Postfach, 4002 Basel oder per E-Mail an: pk.novartis@novartis.com.

5. Datenqualität und -aktualität

Die Versicherungsberatung Novartis trifft geeignete qualitätssichernde Massnahmen, um die Richtigkeit der bearbeiteten Personendaten zu gewährleisten.

- Zu den jeweiligen Providern ist ein Datenaustausch zu unterhalten, wodurch sichergestellt wird, dass diese Daten stets dem aktuellen Stand entsprechen (z.B. Prämieninkasso im Krankenversicherungsbereich).
- Die Datenbearbeitung erfolgt durch die berechtigten Mitarbeitenden der Versicherungsberatung Novartis.

6. Aufbewahrung

Personendaten werden grundsätzlich nur so lange aufbewahren, wie es notwendig ist, um den Zweck zu erfüllen, für den sie erhoben wurden, oder um gesetzliche oder behördliche Vorschriften einzuhalten. Die Versicherungsberatung Novartis nimmt die Antragsdaten auf, und leitet sie an die entsprechenden Versicherer weiter. Nicht mehr benötigte Daten werden umgehend vernichtet.

Papierunterlagen sind so zu vernichten, dass sie nicht rekonstruiert werden können. Gegebenenfalls sind die Unterlagen durch spezialisierte Anbieter in verschlossenen Containern abholen und überwacht entsorgen zu lassen.

7. Schutz vor Fremdzugriff und Vernichtung (Informationssicherheit)[4]

7.1 Zutrittskontrolle

- Die Räume der Versicherungsberatung Novartis sind besonders gesichert.
- Elektronische Daten dürfen nur auf Servern der Novartis in gesicherten, nicht öffentlich zugänglichen Rechenzentren mit gesichertem Zutrittsystem abgelegt werden.
- Diese Rechenzentren sind nur befugten Mitarbeitern zugänglich.

7.2 Zugriffskontrolle

- Die Erteilung von Zugriffsrechten auf Personendaten sowie IT-Systeme ist restriktiv zu handhaben. Die Kompetenz hierzu liegt beim Geschäftsführer der Pensionskasse Novartis.
- Nicht benutzte Accounts sind zu löschen.
- In den Räumen der Versicherungsberatung Novartis ist dafür zu sorgen, dass Besuchern kein unautorisierter Dateneinblick, weder am Bildschirm noch auf Papierdossiers, möglich ist.
- Es gelten die Richtlinien der Novartis über die Passwort-Sicherheit.
- Im Einklang mit den einschlägigen IT-Standards der Novartis sind die Zugriffspasswörter im vorgeschriebenen Zyklus zu ändern.

7.3 Benutzerkontrolle

- Der Zugriff auf die elektronisch, wie auch in Papierform aufbewahrten Daten ist den berechtigten Mitarbeitenden der Versicherungsberatung vorbehalten.

7.4 Weitergabekontrolle[5]

- Daten, die via Schnittstellen oder auf andere Weise übermittelt werden, dürfen nur den hierfür autorisierten Stellen im Rahmen ihrer zweckbestimmten Aufgabe gesichert zugestellt werden. Über die Weitergabe ist Protokoll zu führen.
- Analoges gilt für den Datenaustausch mit Dritten im Auftragsverhältnis.
- Klassifizierte Datenträger müssen als solche gekennzeichnet werden (z.B. „vertraulich“ bzw. „persönlich“). Sie sind entsprechend zu verpacken und zu adressieren.
- Es gelten die Novartis Richtlinien zur sicheren Nutzung von Fax, Internet etc). Mail mit vertraulichen Daten sind per „Secure Novartis Mailsystem“ zu versenden.

[4] Zur Informationssicherheit s. auch Anhang 2 zu diesem Reglement
[5] Zur Weitergabe von Daten an Dritte s. Ziff. 9 f. dieses Reglements

7.5 Eingabekontrolle

- Die Datenbearbeitung erfolgt durch berechtigte Mitarbeitende der Versicherungsberatung entweder über die Schnittstelle oder manuell.

7.6 Auftragskontrolle:

- Wird die Bearbeitung von Personendaten an Dritte vergeben (Outsourcing), sind diese vertraglich, z.B. mittels besonderer Abreden in den einschlägigen Service Level Agreements, zur Einhaltung der Datenschutzanforderungen der Auftraggeberin zu verpflichten.
- Die Versicherungsberatung Novartis behält sich als Auftraggeberin entsprechende Kontrollbefugnisse vor und nimmt diese gebührend wahr, beispielsweise durch Einsichtnahme in die einschlägigen Reglemente und internen Weisungen der Drittpartei.

7.7 Verfügbarkeits-Kontrolle

- Serverräume sind gegen äussere Einflüsse geschützt.
- Backup (automatisch und täglich) und das Rücklesen der Daten sind regelmässig zu testen.
- Der Serverinhalt wird mittels eines virtuellen Backup-Servers gesichert, wobei der virtuelle Server nicht im gleichen Rechenzentrum stehen darf.
- Die Daten sind so sichern, dass sie auch im Fall eines Desasters (Verlust, Vernichtung oder Beschädigung) in nützlicher Frist reproduziert werden können (tägliche Datenspiegelung).

7.8 Trennungskontrolle

- Daten dürfen nur im Rahmen des Leistungsauftrags der Versicherungsberatung Novartis erhoben werden.
- Es besteht kein Zugriff auf die Datensammlung der Pensionskasse Novartis.

7.9 Weitere Kontrollen und Weisungen

- Besonders schützenswerte Daten werden beim Verlassen des Büros in entsprechende Aktenschränke verschlossen.
- Beim Verlassen des Büros gilt eine Clear Desk Policy.
- Der Bildschirm ist beim kurzfristigen Verlassen des Büros zu sichern (Passwort-geschützt).
- Die Festplatte des Notebooks wird encrypted.

8. Datenschutz-„Awareness“

Regelmässige Schulungen für die Mitarbeitenden der Versicherungsberatung Novartis soll Verständnis für die Belange des Datenschutzes schaffen, für Probleme sensibilisieren und die Einhaltung der diesbezüglichen Anforderungen (Compliance) sicherstellen. Die Mitwirkung an den von der Novartis angebotenen, interaktiven Awareness-Tests ist Pflicht. Der Besuch externer Weiterbildungskurse wird unterstützt.

9. Weitergabe von Daten an Dritte

- Personendaten dürfen nur im Rahmen des Leistungsauftrags oder aufgrund ausdrücklicher schriftlicher Einwilligung der betroffenen Person an Dritte weitergegeben werden. Als Drittpartei gilt auch der Lebens- oder Ehepartner der betroffenen Person. Schriftlich erteilte Einwilligungen bzw. Vollmachten gelten bis auf Widerruf.
- Auftragnehmer der Versicherungsberatung Novartis, die in einem besonderen, gesetzlich vorgesehenen Mandatsverhältnis zu ihr stehen, wie z.B. die Kontrollstelle, unterliegen prinzipiell derselben Schweige- und Datenschutzpflicht wie die Auftraggeberin. Dennoch sind die im Rahmen und zur Erfüllung der entsprechenden Mandate weiter gegebenen Personendaten soweit wie möglich zu anonymisieren.
- Für die Weitergabe von Daten an interne Stellen der Novartis (z.B. *People & Organization, Rewards*) ist die Einwilligung der betroffenen Person erforderlich. Kann die Zustimmung in dringenden Fällen nicht eingeholt werden, ist die Datenbekanntgabe gegebenenfalls und ausnahmsweise dennoch möglich, sofern angenommen werden darf, dass die Bekanntgabe im wohlverstandenen Interesse der versicherten Person liegt.

10. Grenzüberschreitender Datentransfer

Die Daten werden prinzipiell der betroffenen Person zur Weiterleitung zugestellt, es sei denn, diese autorisiert ausdrücklich einen Direkttransfer. Die entsprechenden Richtlinien der Novartis über den grenzüberschreitenden Datenaustausch sind anzuwenden.

Für die Übermittlung personenbezogener Daten zwischen Tochtergesellschaften und verbundenen Unternehmen von Novartis hat Novartis die Binding Corporate Rules eingeführt. Dabei handelt es sich um ein System von Grundsätzen, Regeln und Instrumenten, die durch europäisches Recht genehmigt wurden, um die Übermittlung personenbezogener Daten ausserhalb des EWR und der Schweiz zu regeln. Klicken Sie hier, um mehr über die verbindlichen Unternehmensregeln von Novartis zu erfahren.

11. Diverses

11.1 Internes Audit

Zur Durchführung periodischer interner Audits wird der Datenschutzbeauftragte der Pensionskasse Novartis beigezogen. Die Prüfpunkte werden aufgrund einer unfassenden Checkliste gemeinsam festgelegt, die Prüfungsergebnisse protokolliert.

11.2 Homepage der Versicherungsberatung

Die Versicherungsberatung verfügt über eine eigenen elektronischen Internet-Auftritt.

http://www.versicherungsberatung-novartis.ch

Diese dient einzig der **allgemeinen Information** und enthält keine Angaben, die Rückschlüsse auf einzelne Versicherungsnehmer/-innen zulassen.