# Datenschutzreglement der Pensionskassen Novartis

## Ziel

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

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

Als Vorsorgeeinrichtung einer renommierten Stifterfirma behandelt die Pensionskasse Novartis den Schutz von Personendaten ihrer Versicherten mit besonderer Sorgfalt. Die *Data Privacy Policy* sowie die einschlägigen *Key-Directives, Guidelines & Instructions* der Stifterfirma sind auch für die Pensionskasse Novartis 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 gesetzlichen, statutarischen und reglementarischen Bestimmungen und nur für den erklärten Zweck, d.h. für die Durchführung der beruflichen Vorsorge zulässig.

---

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

[2] GPOL-8107309 (novartis.net)

[3] S. Anhang 1 zu diesem Reglement

## 2. Personendaten („Datensparsamkeit“)

Die Pensionskasse Novartis erhebt nur Daten, die zur Zweckerfüllung auf der Grundlage der gesetzlichen, statutarischen und reglementarischen Aufgaben erforderlich sind. Diese Daten sind in der Regel im Versicherungsausweis enthalten und entsprechen somit zugleich den einschlägigen Informationspflichten des BVG:

- Name, Vorname
- Geburtsdatum, Todesdatum
- Geschlecht
- Zivilstand
- Adressen
- E-Mail / Telefonnummer
- Personalnummer (Identifikations-Merkmal zum Personaldatensystem)
- Sprachen
- Lohnfirma
- AHV-Nummer
- Sozialversicherungsnummer
- Mitarbeiterkategorie
- Eintritt in Firma und Kasse
- Beschäftigungsgrad
- Massgebendes Gesamteinkommen
- Vermögen/Kapital
- Incentive/Bonus
- Schichtzulage
- Eheschliessungs-/Scheidungsdatum
- Vorbezugs-/Verpfändungsdaten (WEF/Scheidung)
- Einkaufsleistungen
- Zuzugsdatum
- Freizügigkeitsleistungen
- Anwartschaftliche Alters- und Risikoleistungen
- Beitragsdaten
- Begünstigungsabreden

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 Gesundheitserklärungen, medizinische Gutachten, Einsicht in Akten der IV sowie anderer Sozialversicherungsträger u. dgl.) sind ausschliesslich im Rahmen der Besorgung der gesetzlichen, statutarischen und reglementarischen Aufgaben zu erheben, zu verwenden und mit besonderer Sorgfalt aufzubewahren.

## 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 Pensionskasse Novartis trifft geeignete qualitätssichernde Massnahmen, um die Richtigkeit der bearbeiteten Personendaten zu gewährleisten.

- Zu den jeweiligen Systemen der Stifterfirma ist eine Datenschnittstelle zu unterhalten, wodurch sichergestellt wird, dass die Daten der Pensionskasse stets dem aktuellsten Stand entsprechen und umgekehrt auch die Stifterfirma stets über die aktuellsten pensionskassenspezifischen Daten (Beiträge, Leistungen) verfügen kann. Zudem können die Daten von der versicherten Person jederzeit selbst aktualisiert werden.
- Die Datenbearbeitung erfolgt durch die berechtigten Mitarbeitenden der Geschäftsstelle.

## 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.
Werden Vorsorgeleistungen ausgerichtet, beträgt die Aufbewahrungspflicht bis zehn Jahre nach Beendigung der Leistungspflicht. Werden mangels Geltendmachung durch die versicherte Person keine Vorsorgeleistungen ausgerichtet, so besteht eine Aufbewahrungspflicht bis zum Zeitpunkt, an dem die versicherte Person ihr 100. Altersjahr vollendet hat oder vollendet hätte.

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

### 7.1 Zutrittskontrolle

- Die Räume der Pensionskasse Novartis sind besonders gesichert
- Elektronische Daten dürfen nur auf Servern der Stifterfirma 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 das IT-Verwaltungssystem der Pensionskasse Novartis ist restriktiv zu handhaben. Die Kompetenz hierzu liegt beim Geschäftsführer.
- Nicht benutzte Accounts sind zu löschen.
- In den Räumen der Pensionskasse Novartis ist dafür zu sorgen, dass Besuchern kein unautorisierter Dateneinblick möglich ist.
- Es gelten die Richtlinien der Stifterfirma über die Passwort-Sicherheit.
- Im Einklang mit den einschlägigen IT-Standards der Stifterfirma sind die Zugriffspasswörter im vorgeschriebenen Zyklus zu ändern.

[4] Zur Informationssicherheit s. auch Anhang 2 zu diesem Reglement

### 7.3 Benutzerkontrolle

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

### 7.4 Weitergabekontrolle[5]

- Daten, die via Schnittstellen an die Stifterfirma übermittelt werden, dürfen nur den hierfür autorisierten Stellen im Rahmen ihrer zweckbestimmten Aufgabe (Beitragsbelastung, Rentenauszahlung) zugestellt werden.
- Klassifizierte Datenträger müssen als solche gekennzeichnet werden (z.B. „vertraulich“ bzw. „persönlich“). Sie sind entsprechend zu verpacken und zu adressieren.
- Es gelten die von der Stifterfirma erlassenen Richtlinien zur sicheren Nutzung von Fax, Internet etc. Mail mit vertraulichen Daten sind per „Secure Novartis Mailsystem“ zu versenden.

### 7.5 Eingabekontrolle

- Die Datenbearbeitung erfolgt durch berechtigte Mitarbeitende der Geschäftsstelle entweder über die Schnittstelle oder manuell. Die Eingaben werden protokolliert (Logbuch).

### 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 Pensionskasse 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 Verfügbarkeitskontrolle

- Für den Fall einer Pandemie oder anderer Anwendungsfälle im Rahmen der *Emergency & Business Continuity* Planung der Pensionskasse sind die Zugriffscodes im pensionskasseneigenen Safe hinterlegt und besonders gesichert.
- 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 zu sichern, dass sie auch im Fall eines Desasters (Verlust, Vernichtung oder Beschädigung) in nützlicher Frist reproduziert werden können (tägliche Datenspiegelung).

---

[5] Zur Weitergabe von Daten an Dritte s. Ziff. 9 f. dieses Reglements

### 7.8 Trennungskontrolle

- Es dürfen die erhobenen Daten nur zum Zweck der Durchführung der beruflichen Vorsorge der Pensionskasse Novartis erhoben werden.
- Das Disaster- und Testsystem verfügt über eine eigene Datenbank.

### 7.9 Weitere Kontrollen und Weisungen

- Es gilt eine Clear Desk Policy.
- Der Bildschirm ist beim kurzfristigen Verlassen des Büros zu sichern (Passwort-geschützt)
- Die Festplatte des Notebooks ist encrypted.

## 8. Datenschutz-„Awareness“

Regelmässige Schulungen für die Mitarbeitenden der Pensionskasse 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 Stifterfirma angebotenen, interaktiven Awareness-Tests ist Pflicht. Der Besuch externer Weiterbildungskurse wird unterstützt.

## 9. Weitergabe von Daten an Dritte

- Personendaten dürfen nur im gesetzlichen Rahmen (Art.86a BVG, ggf. in Verbindung mit der allgemeinen Verwaltungshilfebestimmung gemäss Art.32 ATSG) oder aufgrund ausdrücklicher schriftlicher Einwilligung der betroffenen Person an Dritte weitergegeben werden. Als Drittpartei gilt auch der Lebens- oder Ehepartner der versicherten Person. Schriftlich erteilte Einwilligungen bzw. Vollmachten gelten bis auf Widerruf.
- Auftragnehmer der Pensionskasse Novartis, die in einem besonderen, gesetzlich vorgesehenen Mandatsverhältnis zu ihr stehen, wie z.B. Experte für berufliche Vorsorge, Kontrollstelle oder Rückversicherer, unterliegen prinzipiell derselben Schweige- und Datenschutzpflicht wie die auftraggebende Vorsorgeeinrichtung. 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 Stifterfirma (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 (z.B. für konzerninterne Übertrittsberechnungen, im Zusammenhang mit der Suche nach optimierten Vorsorgelösungen für im Falle von Aufhebung des Arbeitsvertrags, Vorruhestand, externer Versicherungsmöglichkeit etc.).
- Ebenfalls zulässig ist die Weitergabe konkreter Versichertendaten, wenn diese von der Stifterfirma benötigt werden, um ihrerseits bestimmten gesetzlichen

Informationspflichten nachkommen zu können (z.B. SWX, Geschäftsbericht, Annual Report, und ähnlichen öffentlichen Berichten).

- Daten, die von der Stifterfirma zur Erstellung von Dokumentationen und Übersichtsbroschüren für die betroffene Person selbst benötigt werden (*Total Compensation Report*), dürfen weitergegeben werden, sofern das Einverständnis der betroffenen Person schlüssig dargelegt werden kann.

## 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 Stifterfirma 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 Pensionskassen Novartis

Die Pensionskassen Novartis verfügen über einen eigenen elektronischen Internet-Auftritt.

http://www.pensionskassen-novartis.ch

Dieser dient einzig der allgemeinen Information und enthält keine Angaben, die Rückschlüsse auf einzelne Versicherte zulassen.