

9. Wir sind für die Einhaltung dieser Grundregeln zum Datenschutz und der geltenden Gesetze, die die Vertraulichkeit persönlicher Mitarbeiterdaten schützen, verantwortlich.

Alle Mitarbeiter, die persönliche Daten anderer Mitarbeiter bearbeiten, sind verpflichtet, diese Grundregeln und alle geltenden Gesetze zum Schutz persönlicher Mitarbeiterdaten zu beachten. Mitarbeiter, die diese Grundregeln oder geltendes Recht verletzen, unterliegen disziplinarischen Maßnahmen, die bis zur Beendigung des Beschäftigungsverhältnisses reichen können.

Wir stellen Aufklärungsprogramme und -schulungen zur Verfügung, die der Information der Mitarbeiter über die Bedeutung und die Anforderungen dieser Grundregeln zum Datenschutz und der geltenden Gesetze dienen.

Mitarbeiter, die Kenntnis von der Verletzung dieser Grundregeln erlangen, müssen Ihren Vorgesetzten, einen Personalrepräsentanten, einen Compliance-Beauftragten oder die Stryker Ethik-Hotline informieren. Soweit möglich, werden wir diese Meldungen vertraulich behandeln.

Wir werden darüber hinaus unsere Datenschutzmaßnahmen intern bewerten und regelmäßig externe Experten mit der Überprüfung der Einhaltung unserer Grundregeln zum Datenschutz und aller geltenden Gesetze sowie der jeweiligen Richtlinien und Vorgehensweisen, die diese Grundregeln stützen, beauftragen.

Mit wem Sie Kontakt aufnehmen können, wenn Sie eine Frage oder eine Beschwerde haben:

Wenn Sie eine Frage zu diesen Grundregeln zum Datenschutz oder zu den Vorgehensweisen in Bezug auf diese Grundregeln haben oder wenn Sie in Bezug auf den Schutz persönlicher Daten eine Beschwerde haben, nehmen Sie bitte Kontakt mit Ihrem Personalrepräsentanten, einem Compliance-Beauftragten oder der Rechtsabteilung auf.

Grundregeln zum Schutz von Mitarbeiterdaten

Unternehmensrichtlinie Nummer Elf



**Copies of all Corporate Policies
may be found on
www.stryker.com/corporatepolicies**

2825 Airview Boulevard
Kalamazoo, MI 49002
t: 269 385 2600 f: 269 385 1062

Zweck:

Die Festlegung der Grundregeln, die für den Schutz der persönlichen Daten unserer Mitarbeiter, die im Rahmen des Beschäftigungsverhältnisses gesammelt werden, gelten.

Geltungsbereich:

Diese Richtlinie gilt für alle Stryker-Mitarbeiter an allen Stryker-Standorten, soweit sie dem geltenden Recht entspricht. Für den Fall, dass einzelne Klauseln dieser Richtlinie nicht dem für eine bestimmte Stryker-Geschäftseinheit geltenden Recht entsprechen, wird diese Geschäftseinheit diese Richtlinie zur Anpassung an örtlich geltendes Recht überarbeiten und/oder eine zusätzliche Richtlinie zur Anpassung an örtlich geltendes Recht erlassen, vorausgesetzt, die überarbeitete Richtlinie erfüllt soweit wie möglich die in dieser Richtlinie enthaltenen Grundregeln. Alle Klauseln dieser Richtlinie, die mit dem örtlich geltenden Recht im Einklang stehen, bleiben gültig.

Präambel:

Wir bei Stryker glauben an den Schutz persönlicher Daten und insbesondere an den Schutz der Daten, die im Rahmen des Beschäftigungsverhältnisses erfasst werden. Wir sind uns auch des großen Vertrauens bewusst, das unsere Mitarbeiter in Strykers verantwortlichen Umgang mit ihren Daten haben. Wir haben diese allgemeinen Grundregeln eingeführt, damit unsere Vorgehensweisen bei Erfassung, Nutzung, Freigabe und Aufbewahrung sowie die Genauigkeit und Sicherheit der bei uns verwahrten persönlichen Daten über potenzielle, derzeitige und ehemalige Mitarbeiter daran ausgerichtet werden.

Unsere Mitarbeiter spielen eine wichtige Rolle für den Schutz dieser Daten, da sie diese Grundregeln beachten müssen. Wir erwarten darüber hinaus, dass die Mitarbeiter uns dabei unterstützen, sicherzustellen, dass die persönlichen Daten, die wir über sie haben, richtig und aktuell sind.

Durch die Befolgung dieser Grundregeln verpflichten wir uns, die geltenden Gesetze und Bestimmungen zum Schutz persönlicher Daten in den Ländern, in denen wir geschäftlich aktiv sind, einzuhalten. Zusätzlich können unsere Geschäftsbereiche weltweit gesonderte Richtlinien erstellen und pflegen, um dem örtlichen Recht zu genügen. Diese örtlich gültigen Richtlinien stimmen jedoch mit den Fair Information Practices überein, den weltweit gültigen Praxisstandards, die als Basis für diese Grundlagen dienen.

Grundregeln:

1. **Wir erfassen, nutzen und bewahren Daten auf, die relevant und wichtig sind.**

Wir begrenzen die Erfassung, Nutzung und Aufbewahrung persönlicher Daten über Mitarbeiter auf den Umfang, der für die Verwaltung der Sozialleistungen für Mitarbeiter, Beschäftigungsaktivitäten und -dienstleistungen, die Erreichung legitimer Geschäftsziele und die Erfüllung gesetzlicher Anforderungen notwendig und wichtig ist.

Wir halten diese Daten nur so lange vor, wie wir sie benötigen oder dies durch Gesetze oder Bestimmungen erforderlich ist.

2. **Wir sagen unseren Mitarbeitern, welche Arten persönlicher Daten wir erfassen und für welche Zwecke wir diese Daten nutzen.**

Wir sagen Bewerbern und neuen Mitarbeitern, welche Arten persönlicher Daten wir von Ihnen erfassen, woher diese Daten stammen, an wen diese Daten weitergegeben werden können sowie für welche mit der Beschäftigung in Zusammenhang stehenden und legitimen Geschäftszwecke wir die Daten erfassen, nutzen und aufbewahren.

3. **Wir holen das Einverständnis des Mitarbeiters für die Erfassung, Nutzung und Offenlegung persönlicher Daten ein, wenn der Mitarbeiter das Recht hat, die Herausgabe dieser persönlichen Daten zu verweigern.**

In vielen Fällen sind die persönlichen Daten für das Beschäftigungsverhältnis oder die Einhaltung von Gesetzen erforderlich, weswegen ein ausdrückliches Einverständnis für die Erfassung und Nutzung solcher Daten nicht erforderlich ist. Wenn jedoch das Einverständnis des Mitarbeiters für die Erfassung oder Weitergabe persönlicher Daten eingeholt werden muss, um dem Mitarbeiter bestimmte Leistungen anbieten zu können, werden wir das Einverständnis des Mitarbeiters einholen.

4. **Wir sorgen dafür, dass Mitarbeiterdaten vollständig, richtig und aktuell vorliegen.**

Wir treffen angemessene Vorkehrungen, um sicherzustellen, dass die von uns erfassten und genutzten persönlichen Daten über Mitarbeiter vollständig, richtig und aktuell sind. Wir ergreifen angemessene Maßnahmen, um sicherzustellen, dass Dritte, von denen wir persönliche Daten erhalten, hohe

Qualitätsstandards einhalten. Alle Mitarbeiter sind dafür verantwortlich, uns dabei zu helfen, dass bestimmte Arten persönlicher Daten vollständig, richtig und auf neuestem Stand sind.

5. **Wir sagen den Mitarbeitern, wie sie nachsehen können, welche persönlichen Daten wir von ihnen haben.**

Mitarbeiter können bestimmte persönliche Daten, die bei uns vorliegen, über ihren Personalrepräsentanten einsehen.

6. **Wir schützen die Sicherheit und Vertraulichkeit persönlicher Daten.**

Wir ergreifen angemessene Maßnahmen, um den Zugriff auf persönliche Mitarbeiterdaten auf diejenigen Personen zu beschränken, die auf Grund der mit ihrer Tätigkeit verbundenen Pflichten ein gerechtfertigtes Interesse an diesen Daten haben. Wir unternehmen erhebliche Anstrengungen, um sicherzustellen, dass angemessene administrative, technische und physische Sicherungsmaßnahmen zum Schutz der Vertraulichkeit und Sicherheit persönlicher Daten ergriffen werden.

7. **Wir geben persönliche Mitarbeiterdaten nur dann an Empfänger außerhalb von Stryker weiter, wenn legitime Geschäftszwecke erfüllt werden.**

Wir geben persönliche Daten unserer Mitarbeiter nur dann an Unternehmen außerhalb von Stryker weiter, wenn dadurch legitime Geschäftszwecke erfüllt werden, die durch gesetzliche oder rechtliche Abläufe vorgegeben sind bzw. die die Interessen der Stryker-Mitarbeiter schützen.

8. **Dienstleistungsunternehmen, die für Stryker tätig werden, müssen persönliche Daten von Stryker-Mitarbeitern vertraulich und sicher aufbewahren.**

Wir beauftragen andere Unternehmen häufig damit, in unserem Auftrag Dienstleistungen, wie z. B. die Verwaltung von Ansprüchen aus Krankenversicherungen oder die Gehaltsabrechnung, abzuwickeln. Wir fordern von diesen Unternehmen, dass die von Stryker zur Verfügung gestellten persönlichen Daten ausschließlich für die vereinbarte Nutzungsart verwendet werden und dass die Sicherheit persönlicher Daten gewährleistet wird.