

Name: Safe Harbor Datenschutzrichtlinie für Mitarbeiter	Nummer der Richtlinie: P.01.01
Name der Abteilung: Brunswick Rechtsabteilung	Seite: 1 von 6
Ursprüngliches Veröffentlichungsdatum: 22. April 2013	Änderungsdatum: Nicht zutreffend
Verantwortlich für die Richtlinie: Brunswick Büro für Datenschutz	Ansprechpartner für die Richtlinie: General Counsel (Justiziar)

Zweck und Anwendbarkeit

Diese Safe Harbor („Sicherer Hafen“) Datenschutzrichtlinie für Mitarbeiter von Brunswick (Brunswick Safe Harbor Privacy Policy for Employees) („Richtlinie“) erklärt, wie der Brunswick-Konzern und seine verbundenen Unternehmen („Brunswick“) personenbezogene Daten in Bezug auf Vollzeit- und Teilzeitmitarbeiter mit befristeten und/oder unbefristeten Verträgen, Stellenbewerber, Berater oder Auftragnehmer in den Vereinigten Staaten, im Europäischen Wirtschaftsraum („EWR“) und in der Schweiz erfassen und verarbeiten. Diese Richtlinie gilt für personenbezogene Daten dieser Personen, die in einem beliebigen elektronischen Format vorliegen oder auf elektronischem Weg erfasst wurden.

Jede Person und jede juristische Person, die im Auftrag von Brunswick persönliche elektronische Daten in Bezug auf Datensubjekte in den USA, im EWR oder in der Schweiz erfasst und/oder verarbeitet, muss diese Richtlinie befolgen.

Definitionen

Beauftragter: Jede Person und jede juristische Person, die unter der Leitung von Brunswick personenbezogene Daten verarbeitet; dazu zählen unter anderem Gehaltsabrechnungsdienstleister, Softwareentwickler oder -anbieter, Vermittler von Sozialleistungen, Anbieter von Sozialleistungen, Anbieter von Schulungen, Personalberater, Versicherungsunternehmen sowie Steuer- und Buchhaltungsfirmen.

Datensubjekte: Mitarbeiter, Stellenbewerber, Berater und Auftragnehmer.

Datenerfassungspunkte: Internet, Telefon, Fax, E-Mail oder andere elektronische Systeme, aus denen personenbezogene Daten erfasst werden. Die Erfassungspunkte für Personaldaten können Online-Foren, Fragebögen, Lebensläufe und Stellenbewerbungen, elektronische Aufzeichnungen von Bewerbungsgesprächen/Treffen mit Datensubjekten und/oder Gespräche mit Vorgesetzten und Kollegen sowie Arbeitsverträge in elektronischer Form einschließen.

Mitarbeiter: Mitarbeiter mit befristeten und unbefristeten Arbeitsverträgen, in Vollzeit oder Teilzeit.

Europäischer Wirtschaftsraum (EWR): Österreich, Belgien, Bulgarien, Zypern, die Tschechische Republik, Dänemark, Estland, Finnland, Frankreich, Deutschland, Griechenland, Ungarn, Island, Irland, Italien, Lettland, Liechtenstein, Litauen, Luxemburg, Malta, die Niederlande, Norwegen, Polen, Portugal, Rumänien, Slowakei, Slowenien, Spanien, Schweden, das Vereinigte Königreich von Großbritannien (einschließlich England, Schottland, Nordirland und Wales) und alle anderen

Länder, die später möglicherweise als dem EWR zugehörig betrachtet werden.

Weiterübermittlung: Die Übermittlung von persönlichen Daten an Beauftragte oder Drittparteien, auch das Verfügbarmachen solcher Daten für Beauftragte oder Drittparteien.

Personenbezogene Daten: Elektronische Daten über eine identifizierte oder identifizierbare Person, die durch Brunswick entgegengenommen, erlangt oder verwaltet werden. Zu personenbezogenen Daten zählen (unter anderem): Name, Geburtsdatum, Passnummer, Wohnsitz-Kontaktinformationen, geschäftliche Kontaktinformationen, Familienstand, Informationen zu Familienmitgliedern, Notfall-Kontaktinformationen, Qualifikationen und berufliche Laufbahn, Beschäftigungsbedingungen, Beschäftigungsstatus, Arbeitszeit, Einstellungskategorie, Gehalt, Vorsorgepläne für Mitarbeiter, Anwesenheitsnachweise, Leistungsüberprüfungen, Berichtsstruktur, Hintergrundinformationen (wo gesetzlich zulässig), Informationen zur Steuererklärungspflicht, Mitteilungen zu Disziplinarmaßnahmen und Beschwerden, Fotos von und Informationen zu Ausrüstungsgegenständen, die von Brunswick zur Verfügung gestellt wurden, darunter Telefone, Fahrzeuge und Kreditkarten, sowie ähnliche Informationen.

Verarbeitung: Alle Transaktionen oder Serien von Transaktionen, die mit den personenbezogenen Daten durchgeführt werden, sowohl automatisch als auch manuell. Dazu zählt das Erfassen, Aufbewahren, Aufzeichnen, Organisieren, Speichern, Anpassen oder Verändern, Abrufen, Konsultieren, Verwenden, Offenlegen, Verbreiten oder anderweitig Verfügbarmachen, Sperren, Löschen oder Zerstören von personenbezogenen Daten. Die Verarbeitung schließt auch Tätigkeiten wie das Kopieren, Ablegen und Eingeben von personenbezogenen Daten in eine Datenbank ein.

Safe Harbor („Sicherer Hafen“): Das Department of Commerce (Handelsministerium, „DoC“) der Vereinigten Staaten (USA) und die Europäische Kommission, und das DoC und der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte der Schweiz haben separat voneinander Datenschutzprinzipien vereinbart (gemeinsam bezeichnet als „Safe Harbor-Prinzipien“), um es US-Unternehmen zu ermöglichen, personenbezogene Daten aus dem EWR und der Schweiz unter Einhaltung der europäischen und schweizerischen Gesetze in die USA zu übermitteln. Die Teilnahme an Safe Harbor gestattet es Brunswick, personenbezogene Daten legal aus dem EWR und der Schweiz in die Vereinigten Staaten zu transferieren.

Sensible personenbezogene Daten: Elektronische personenbezogene Daten, die sich auf den medizinischen oder Gesundheitszustand, die Rasse, die nationale Herkunft, auf politische Meinungen oder Zugehörigkeiten, religiöse oder philosophische Bekenntnisse, die Mitgliedschaft in Gewerkschaften oder das Sexualleben eines Datensubjekts beziehen.

Drittpartei: Eine Person oder eine juristische Person, die weder von Brunswick beauftragt noch mit dem Unternehmen verbunden ist, und die nicht im Auftrag von Brunswick oder unter der Leitung von Brunswick agiert.

Safe Harbor

Im Einklang mit seiner Verpflichtung, die Privatsphäre zu schützen, erfüllt Brunswick die Safe Harbor-Rahmenkonzepte zwischen den USA und der EU und zwischen den USA und der Schweiz

und befolgt die Safe Harbor-Prinzipien beider Vereinbarungen. Weitere Information über die Safe Harbor-Prinzipien erhalten Sie auf der Website des Department of Commerce (Handelsministeriums) der USA unter: <http://export.gov/safeharbor/>.

Grundsätze der Richtlinie

- A. **Sicherheit im Unternehmen.** Gemäß dieser Richtlinie und den Datensicherungsverfahren von Brunswick müssen alle Personen, für die diese Richtlinie gilt, die administrativen, technischen und physischen Absicherungsmaßnahmen von Brunswick befolgen, um personenbezogene Daten vor Verlust, Missbrauch, unberechtigtem Zugriff, Offenlegung, Veränderung oder Zerstörung zu schützen.
- B. **Sicherheit bei Beauftragten.** Brunswick kann den Transfer personenbezogener Daten an einen Beauftragten genehmigen, wenn eine der folgenden Bedingungen erfüllt ist:
 - i. der Beauftragte ist unter dem geltenden Safe Harbor-Programm zertifiziert;
 - ii. der Beauftragte unterliegt der EU-Direktive von 1995, den Datenschutzgesetzen des EWR bzw. der Schweiz oder einem äquivalenten Gesetz, dem die Europäische Kommission ein angemessenes Datenschutzniveau attestiert hat; oder
 - iii. der Beauftragte hat eine schriftliche Vereinbarung mit Brunswick abgeschlossen, die das gleiche oder ein höheres Datenschutzniveau vorschreibt, als in dieser Richtlinie beschrieben.
- C. **Sensible personenbezogene Daten.** Sensible personenbezogene Daten dürfen ohne die explizite vorherige Zustimmung des Datensubjekts und die Vorabgenehmigung durch das Büro für Datenschutz weder erfasst, gehandhabt noch verarbeitet werden, sofern nicht durch die geltenden Gesetze anderweitige Festlegungen bestehen bzw. mit Ausnahme der nachfolgend in diesem Dokument beschriebenen Fälle.
- D. **Benachrichtigung.** Mitarbeiter sollten sich mit Fragen oder Beschwerden in Bezug auf die Datensicherheit, den Umgang mit personenbezogenen Daten oder sensiblen personenbezogenen Daten oder Datenerfassungspunkten an das Büro für Datenschutz wenden.
- E. **Einhaltung.** Die Einhaltung der Safe Harbor-Prinzipien (siehe unten) ist obligatorisch. Verletzungen dieser Richtlinie können für Mitarbeiter disziplinarische Maßnahmen, bis hin zu einer Kündigung des Arbeitsverhältnisses, zur Folge haben bzw. die Beendigung der Geschäftsbeziehungen zu Auftragnehmern und Beratern.
- F. **Selbsteinschätzung.** Brunswick wird auf jährlicher Basis Selbsteinschätzungen in Bezug auf die Einhaltung der Safe Harbor-Prinzipien anordnen. Mitarbeiter, Auftragnehmer und Berater müssen die Durchführung von Audits unterstützen, wenn sie dazu aufgefordert werden.

Die Safe Harbor-Prinzipien

Personen, die im Auftrag von Brunswick personenbezogene Daten verarbeiten, müssen die

folgenden Safe Harbor-Prinzipien einhalten:

A. Benachrichtigung.

i. Erfordernisse für Benachrichtigungen. Außer für anonyme oder aggregierte Daten, das heißt Daten, die keine Person identifizieren, wird Brunswick jedem Datensubjekt, von dem die personenbezogenen Daten erfasst wurden, die folgenden Informationen in klarer und deutlicher Sprache zur Verfügung stellen:

1. den Zweck der Erfassung der personenbezogenen Daten (z. B. siehe unten „Verwendungszwecke, für die personenbezogene Daten/Personaldate erfasst werden“);
2. wie man sich mit Anfragen oder Beschwerden an das Büro für Datenschutz wenden kann;
3. die Arten von Beauftragten und Drittparteien, denen gegenüber das Unternehmen die personenbezogenen Daten offenlegt; und
4. die Wahlmöglichkeiten und Mittel, die Brunswick den Datensubjekten bezüglich der Einschränkung der Nutzung und Offenlegung ihrer personenbezogenen Daten bietet.

ii. Wann Benachrichtigungen erfolgen. Brunswick wird eine Benachrichtigung ausgeben, wenn das Unternehmen erstmalig personenbezogene Daten anfordert bzw. sobald es nach diesem Zeitpunkt praktikabel ist. Brunswick wird ebenfalls eine Benachrichtigung ausgeben, bevor das Unternehmen solche Daten für einen anderen Zweck nutzt als jenen, für den die Daten ursprünglich erfasst oder verarbeitet wurden. Für personenbezogene Daten, die von Datensubjekten erfasst wurden, bevor diese Richtlinie in Kraft getreten ist, beschreibt der folgende Abschnitt die Verwendungszwecke, für die solche Daten erfasst wurden:

Verwendungszweck(e), für die personenbezogene Daten/Personaldate erfasst wurden

Berechtigte Personen dürfen personenbezogene Daten unter anderem für die folgenden beschäftigungsbezogenen Zwecke nutzen: (i) Berichterstattung und Statistiken; (ii) Leistungsmanagement und -beurteilung; (iii) Mitarbeitersuche; (iv) Unterstützung der Mobilität der Mitarbeiter; (v) Nachfolgeplanung und Maßnahmen zur Entwicklung qualifizierter Mitarbeiter; (vi) Schulung; (vii) Bearbeitung von Sozialleistungen; (viii) Budgetierung und Prognose; (ix) Buchhaltung und Gehaltsabrechnung; (x) finanzielle Offenlegungen; (xi) Pflege von Datenbanken und Gewährung von IT-Support; (xii) Sicherstellung der Einhaltung der Richtlinien und des Verhaltenskodex von Brunswick, einschließlich, unter anderem, des Ethikprogramms von Brunswick und damit verbundener Untersuchungen; (xiii) Einstellung und Kündigung; (xiv) Personalwesen; (xv) Personalmanagement für Funktionseinheiten von Brunswick; und (xvi) Einhaltung gesetzlicher Verpflichtungen.

B. Wahlmöglichkeit. Brunswick stellt klare und deutliche Benachrichtigungen zur Verfügung, sowie einfach zugängliche und erschwingliche Mechanismen, mit deren Hilfe Datensubjekte

wählen können, wie ihre personenbezogenen Daten unter bestimmten Umständen verarbeitet werden. Datensubjekte können ihre Zustimmung verweigern, wenn ihre personenbezogenen Daten:

1. gegenüber einer Drittpartei offengelegt werden sollen; davon ausgenommen sind die nachfolgend im Abschnitt Weiterübermittlung erläuterten Fälle;
2. für einen Zweck verwendet werden sollen, der nicht mit dem/den Verwendungszweck/en kompatibel ist, für den die Daten ursprünglich erfasst wurden oder der zu einem späteren Zeitpunkt durch die Person genehmigt wurde.

Wenn das Datensubjekt mit der Verarbeitung seiner bzw. ihrer personenbezogenen Daten unter den oben beschriebenen Umständen nicht einverstanden ist (d. h., die Person verweigert ihre Zustimmung), dann können die personenbezogenen Daten für diesen Zweck nicht verarbeitet werden.

C. Sensible personenbezogene Daten

- i. Sensible personenbezogene Daten dürfen nicht erfasst oder offengelegt werden, wenn das Datensubjekt nicht ausdrücklich einwilligt („die Zustimmung dazu gibt“). Ausnahmen sind nachfolgend beschrieben.
- ii. Datensubjekte müssen auch ausdrücklich einwilligen, wenn sensible personenbezogene Daten für einen anderen Zweck verwendet werden sollen, als für jenen, der ursprünglich genehmigt wurde.
- iii. Eine Zustimmung ist nicht erforderlich, wenn die Offenlegung:
 1. gesetzlich oder durch ein Gerichtsverfahren erforderlich ist;
 2. notwendig oder angemessen ist, um körperlichen Schaden, die Beschädigung oder den Verlust von Eigentum oder finanziellen Verlust zu verhindern;
 3. mit einer Untersuchung mutmaßlicher oder tatsächlicher illegaler Handlungen oder einer Verletzung der Unternehmensrichtlinie im Zusammenhang steht.

D. Weiterübermittlungen

- i. Brunswick wird die Prinzipien der Benachrichtigung und der Wahlmöglichkeiten (siehe oben) befolgen, bevor das Unternehmen personenbezogene Daten gegenüber einer Drittpartei offenlegt.
- ii. Brunswick wird personenbezogene Daten nur dann an einen Beauftragten weiterübermitteln, wenn der Beauftragte: (i) sich für das Safe Harbor-Programm angemeldet hat; (ii) der EU-Direktive unterliegt; (iii) verbindliche Unternehmensregeln besitzt; (iv) eine schriftliche Vereinbarung unterzeichnet hat, deren gefordertes Datenschutzniveau den Safe Harbor-Prinzipien entspricht oder sie übertrifft, oder anderweitig dem Bundesgesetz über den Datenschutz der Schweiz oder einer sonstigen Feststellung der „Adäquanz“ durch die Europäische Kommission unterliegt.

E. Zugang

- i. Brunswick bietet den Datensubjekten Zugang zu ihren personenbezogenen Daten und wird berechtigten Anträgen auf Korrektur, Änderung oder Löschung von personenbezogenen Daten nachkommen.
- ii. Brunswick kann den Zugang zu personenbezogenen Daten einschränken oder

- verweigern, wenn die Gewährung eines solchen Zugangs unter den gegebenen Umständen unzumutbar aufwändig oder sehr teuer ist, oder wenn dies anderweitig durch die Safe Harbor-Prinzipien zulässig ist.
- iii. Um Zugang zu den personenbezogenen Daten zu erhalten, können Datensubjekte das Datenschutzbüro von Brunswick kontaktieren.

F. Sicherheit

Brunswick unterhält gemäß dieser Richtlinie und den Datensicherungsverfahren des Unternehmens angemessene administrative, technische und physische Absicherungsmaßnahmen, um personenbezogene Daten vor Verlust, Missbrauch, unberechtigtem Zugriff, Offenlegung, Veränderung oder Zerstörung zu schützen. Bitte wenden Sie sich an das Büro für Datenschutz, um weitere Informationen zu erhalten.

G. Datenintegrität:

Alle Personen und juristischen Personen, die dieser Richtlinie unterliegen, müssen angemessene Schritte unternehmen, um sicherzustellen, dass die personenbezogenen Daten, die sie erfassen und/oder verarbeiten, für den beabsichtigten Gebrauch relevant, korrekt, vollständig und aktuell sind. Brunswick ist darauf angewiesen, dass Datensubjekte ihre personenbezogenen Daten bei Bedarf aktualisieren und korrigieren.

H. Durchsetzung:

- i. Brunswick hat Richtlinien und Verfahren eingerichtet, um die Einhaltung der Safe Harbor-Prinzipien regelmäßig zu überprüfen.
- ii. Brunswick wird vor der Beantragung der Safe Harbor-Rezertifizierung beim US-Department of Commerce (US-Handelsministerium) eine jährliche Selbsteinschätzung seiner Datenschutzpraktiken durchführen.
- iii. Datensubjekte können Beschwerden bezüglich der Verarbeitung ihrer personenbezogenen Daten beim Büro für Datenschutz von Brunswick einreichen. Wenn eine Beschwerde in Bezug auf einen mutmaßlichen Verstoß gegen die Safe Harbor-Prinzipien durch einen internen Prozess nicht geklärt werden kann, wird sich Brunswick zur Klärung mit EU-Regierungs- bzw. EU-Aufsichtsbehörden in Verbindung setzen.
- iv. Brunswick wird Schritte unternehmen, um bei Beschwerden oder Anfragen, die aus einer Verletzung der Safe Harbor-Prinzipien resultieren, Abhilfe zu schaffen.

Beschränkung der Anwendung der Prinzipien

Die Befolgung der Safe Harbor-Prinzipien kann eingeschränkt sein, (a) sofern dies erforderlich ist, um einer rechtlichen oder ethischen Verpflichtung nachzukommen, (b) sofern dies erforderlich ist, um Verpflichtungen in Bezug auf die nationale Sicherheit, das öffentliche Interesse oder den Gesetzesvollzug zu erfüllen und (c) sofern dies durch geltende Gesetze, Regelungen oder Vorschriften ausdrücklich genehmigt ist.

Änderungen an dieser Richtlinie

Von Zeit zu Zeit kann diese Richtlinie überarbeitet und/oder ergänzt und entsprechend veröffentlicht und kommuniziert werden. Mitarbeiter sollten sicherstellen, dass sie die Richtlinie mit dem aktuellsten Überarbeitungsdatum einsehen.

Kontaktinformationen des Büros für Datenschutz von Brunswick

E-Mail: privacy@brunswick.com

Telefon: 855-283-1103 (gebührenfrei Nordamerika) oder 847-735-4002

Schriftlich: General Counsel
Privacy Office
1 N. Field Court
Lake Forest, Illinois 60045, USA

Wenn Sie es bevorzugen, für Ihre Fragen und im Kontakt mit dem Büro für Datenschutz Ihre Landessprache zu nutzen, wenden Sie sich bitte an Ihren lokalen Vertreter der Personal- oder Finanzabteilung, der die Verbindung zum Büro für Datenschutz herstellen wird.

Weitere Dokumente in diesem Zusammenhang:

1. Security Policy (Sicherheitsrichtlinie) (I.01.01)
2. Classification of Controlled Data Policy (Richtlinie zur Klassifizierung kontrollierter Daten) (P.01.02)
3. Records Management Policy & Schedule (Richtlinie zum Unterlagenmanagement und Zeitplan) (L.03.01)
4. Protection of Restricted Data Policy (Richtlinie zum Schutz vertraulicher Daten) (I.0.01.10.00)
5. Die Safe Harbor-Zertifizierung(en) von Brunswick finden Sie unter <https://safeharbor.export.gov/list.aspx>.

Verantwortlicher für diese Richtlinie und Kontaktperson

Verantwortlich für die Richtlinie: Brunswick Büro für Datenschutz

Leiter für Datenschutz: General Counsel (Justiziar)