

DATENSCHUTZ GEMÄSS DEN GRUNDSÄTZEN DES SICHEREN HAFENS

GÜLTIG AB: 1. Juli 2005

Diese Erklärung legt die von der United Technologies Corporation und ihren in den USA ansässigen Betriebsgesellschaften, Tochterfirmen, Geschäftsbereichen und Unternehmensgruppen sowie all ihren Rechtsvorgängern und -nachfolgern (im Folgenden „UTC“) befolgten Grundsätze im Zusammenhang mit der Übermittlung von personenbezogenen Mitarbeiterdaten (Personaldaten) in die USA von Standorten innerhalb der Mitgliedsstaaten des Europäischen Wirtschaftsraums („EWR“) aus dar. UTC hält die von der Europäischen Kommission (gemäß Entscheidung 520/2000/EG vom 26. Juli 2000) genehmigten *Safe Harbor-Grundsätze (Grundsätze des sicheren Hafens)* des US Department of Commerce ein.

In dieser Erklärung werden folgende Definitionen verwendet:

- „Personenbezogene Mitarbeiterdaten“ bedeuten Daten über identifizierte bzw. identifizierbare UTC-Mitarbeiter, die als digitale Akten in relevanten Ablagesystemen gepflegt werden. Die Definition umfasst Informationen, die bei entsprechender Zuordnung zu einem Mitarbeiter zur Identifizierung dieses Mitarbeiters verwendet werden können. Hierzu zählen beispielsweise folgende Informationen: Anschrift, Telefonnummer, Geschlecht, Geburtsdatum, Lohn- und Gehaltsunterlagen, Telefon- und Telekommunikationsbelege und Leistungsbewertungen. Zu statistischen, historischen und wissenschaftlichen oder sonstigen Zwecken verwendete anonyme Informationen sind hiervon ausgenommen.
- „Schutzwürdige Mitarbeiterdaten“ sind personenbezogene Daten zu Mitarbeitern. Hierzu zählen medizinische Unterlagen, Zugehörigkeit zu bestimmten Rassen oder ethnische Herkunft, politische Ansichten, religiöse oder philosophische Überzeugungen, Mitgliedschaft in Gewerkschaften oder Sexualleben.
- „Vertreter“ bezieht sich auf Dritte, die zur Ausübung bestimmter Aufgaben im Namen von UTC und unter UTCs Anleitung von UTC zur Verfügung gestellte personenbezogene Mitarbeiterdaten benutzen.

GELTUNGSBEREICH

Diese Erklärung bezieht sich, unabhängig von der Übermittlungsform (einschließlich elektronischer, schriftlicher und mündlicher Informationen), auf alle Übermittlungen personenbezogener UTC-Mitarbeiterdaten in die USA von Standorten innerhalb des Europäischen Wirtschaftsraums (EWR) aus. Dabei ist es unerheblich, ob diese Übermittlung über Telekommunikations- oder Computerverbindungen oder im Druckformat erfolgt, und unabhängig davon, ob diese Informationen von UTC und seinen Betriebsgesellschaften oder sonstwie von Vertretern oder sonstigen Dritten erstellt worden sind.

ERFASSUNG, NUTZUNG UND SPEICHERUNG VON PERSONENBEZOGENEN MITARBEITERDATEN

UTC erfasst, nutzt und speichert personenbezogene Mitarbeiterdaten nur dann, wenn solche Informationen für legitime Geschäfts- und rechtliche Zwecke erforderlich sind.

Wenn UTC personenbezogene Daten direkt von Mitarbeitern im EWR erfasst, informiert das Unternehmen alle Betroffenen über den Zweck dieser Datenerfassung und deren Nutzung, über die Art von Drittparteien, die keine UTC-Vertreter sind und denen UTC diese Informationen übermittelt, sowie über die Möglichkeiten und Mittel, die UTC zur Beschränkung der Nutzung und Preisgabe dieser Daten anbietet. Wenn Mitarbeiter gebeten werden, UTC derartige Informationen zur Verfügung zu stellen, werden sie zu diesem Zeitpunkt bzw. so bald wie möglich danach in klarer, deutlicher Sprache in Kenntnis gesetzt. Auf jeden Fall erfolgt die Inkenntnissetzung, bevor UTC die Informationen zu anderen Zwecken als denen nutzt, für die diese Informationen ursprünglich erfasst wurden.

Wenn UTC von seinen Tochtergesellschaften, verbundenen Unternehmen, Vertretern oder sonstigen Organisationen im EWR personenbezogene Mitarbeiterdaten erhält, werden diese Informationen im Einklang mit den von diesen Organisationen bereitgestellten Erklärungen und den von den betroffenen Mitarbeitern gewählten Optionen genutzt.

Personenbezogene Daten zu individuellen Mitarbeitern werden, sofern durch Gesetze, Verordnungen/Vorschriften oder gerichtliche Verfügungen erlaubt oder vorgeschrieben, an andere UTC-Geschäftsbereiche, Tochtergesellschaften, verbundene Unternehmen, UTC-Vertreter (beispielsweise IT- und sonstige Fach- und andere Dienstleister, Sozialleistungsträger und -verwalter usw.), befugte Regierungsorganisation und Behörden sowie entsprechend befugte Dritte weitergegeben und gemeinsam genutzt.

Die Nutzungszwecke umfassen Folgendes:

- Management- und Mitarbeiterkommunikation und -mitteilungen,
- Pflege von Direktoren- und Mitarbeiterbiografien, -lebensläufen und ähnlichen Informationen,
- Kontaktdaten für Notfälle,
- globale Personalzahlen und demographische Statistiken,
- Karriereentwicklung, Leistungsfeedback und Aufstiegsmöglichkeiten,
- Personalplanung,
- Nachfolgeplanung,
- Vergütung und Nebenleistungen,
- Einrichtung und Verwaltung von Sozial- und -Nebenleistungsplänen für Mitarbeiter,
- Belohnungen und Anerkennungen,
- Erstattung von Reise- und sonstigen Aufwendungen und/oder Kreditkartenverwaltung,
- Schulungen,
- Versetzungen,
- Steuerbezogene Meldungen Reporting und Steuereinbehaltungen,
- Lohn- und Gehaltsabrechnungen, einschließlich Abzügen, Zuschüssen usw.,
- Industrial Relations, einschließlich Schlichtungsverfahren,
- Identifizierung von Personen anhand von Fotos oder sonstigen Bilder,
- Planung und Bereitstellung von Gesundheitsleistungen, einschließlich Drogenscreening, sowie Administration von Betriebsunfallversicherungen und ähnlichen Gesundheits- und Sicherheitsprogrammen,
- persönliche Sicherheitsmaßnahmen wie Zugriffskontrollen und Sicherheitseinrichtungen für Computer- und sonstige Systeme,
- Reporting und statistische Analysen,
- zugehörige Personaltransaktionen,
- gesetzlich vorgeschriebenes Reporting an Behörden, darunter Berichte über Umgebungsbedingungen, Gesundheit und Sicherheit am Arbeitsplatz sowie Verwaltung,
- Visa, Lizenzen und sonstige Arbeitsgenehmigungen,
- Ein- und Ausfuhrkontrolle,
- Interne und externe Untersuchungen, darunter Überprüfungen der Geschäftspraktiken, DIALOG-Programme und Kontakte zu UTC-Ombudsleuten, Überwachung von Internet, Intranet, E-Mail und sonstigen elektronischen Einrichtungen, Anfragen von Polizei- und sonstigen Behörden und
- Unternehmensplanung, einschließlich Verfolgung von Fusionen, Übernahmen und Ausgliederungen.

OPT-OUT/OPT-IN

UTC bietet seinen Mitarbeitern die Möglichkeit des Opt-Out, das heißt, sie können bestimmen, ob ihre personenbezogenen Daten (a) Dritten, die keine UTC-Vertreter sind, mitgeteilt werden und ob diese Daten (b) zu anderen Zwecken als denen genutzt werden, für die sie ursprünglich erfasst wurden. UTC kann seine Mitglieder gelegentlich über Angebote von ausgewählten Drittparteien, die keine UTC-Vertreter sind, informieren; jedoch übermittelt UTC ohne Zustimmung des jeweiligen Mitarbeiters keine personenbezogenen Daten an derartige Drittparteien.

Bei schutzwürdigen personenbezogenen Daten gibt UTC Mitarbeitern die Möglichkeit des Opt-In, das heißt, sie können vor (a) der Übermittlung von Informationen an Drittparteien, die nicht UTC-Vertreter sind, oder (b) der Nutzung von Informationen zu anderen Zwecken als denen, für die sie ursprünglich erfasst oder später freigegeben wurden, dieser Übermittlung deutlich und ausdrücklich zustimmen. Mitarbeiter, die die Opt-In-Möglichkeit wählen, werden über den anzuwendenden Prozess für diese Wahlmöglichkeit in Kenntnis gesetzt.

DATENINTEGRITÄT

UTC nutzt personenbezogene Mitarbeiterdaten nur in einer Art und Weise, die mit den Zwecken, für die diese Daten ursprünglich erfasst und später freigegeben wurden, im Einklang steht. UTC unternimmt angemessene Schritte, um sicherzustellen, dass personenbezogene Daten für den beabsichtigten Zweck relevant, richtig, vollständig und aktuell sind.

ÜBERMITTLUNG AN VERTRETER

UTC lässt sich von seinen Vertretern zusichern, dass sie personenbezogene Mitarbeiterdaten im Einklang mit dieser Erklärung schützen. Beispiele für angemessene Zusicherungen umfassen Folgendes: einen Vertrag, eine Vereinbarung oder eine Klausel, die den Vertreter verpflichtet, mindestens den gleichen Schutz zu gewähren, wie er in den relevanten *Grundsätzen des sicheren Hafens* gefordert wird, eine *Safe Harbor-Zertifizierung* des Vertreters oder ein „Adequacy Finding“ (Feststellung der Angemessenheit) der Europäischen Kommission. Wenn UTC Kenntnis erlangt, dass ein Vertreter personenbezogene Mitarbeiterdaten auf eine Art und Weise nutzt oder preisgibt, die dieser Erklärung zuwiderläuft, unternimmt UTC angemessene Schritte, um diese Nutzung oder Preisgabe zu verhindern bzw. zu unterbinden.

ZUGRIFF UND KORREKTUR

Auf Verlangen gewährt UTC seinen Mitarbeitern angemessenen Zugriff auf ihre personenbezogenen Daten. Außerdem unternimmt UTC angemessene Schritte, um seinen Mitarbeitern die Möglichkeit zur Korrigierung, Ergänzung oder Löschung von Informationen zu geben, die nachweislich falsch oder unvollständig sind. Beispielsweise erlaubt das Employee Self-Service-System (ESS) den Mitarbeitern, ihre eigenen Akten einzusehen und bei Bedarf zu aktualisieren bzw. zu korrigieren.

SICHERHEIT

UTC setzt Systeme und Verfahren ein, die die Sicherheit und Integrität von personenbezogenen Mitarbeiterdaten schützen, gleichgültig ob diese Daten von den Mitarbeitern selber zur Verfügung gestellt, von UTC und seinen Betriebsgesellschaften erstellt oder sonstwie von seinen Vertretern oder Drittparteien bereitgestellt wurden.

UTC setzt angemessene Vorsichtsmaßnahmen ein, um die in seinem Besitz befindlichen personenbezogenen Daten gegen Verlust, Missbrauch, unbefugten Zugriff, Preisgabe, Manipulierung oder Löschung zu schützen. Gemäß den UTC Information Technology Security Policies (Sicherheitsrichtlinien für Informationstechnologie) sind UTCs Computernetzwerke und -systeme, einschließlich ESS und dessen Internet- und Intranet-basierte Anwendungen, so ausgelegt, dass personenbezogene Mitarbeiterdaten gegen unbefugten Zugriff, Verlust, Preisgabe und Nutzung geschützt sind. Personenbezogene Mitarbeiterdaten werden bei UTC nur auf Need-to-know-Basis zur Verfügung gestellt.

UTC betrachtet das Internet und sonstige Technologien als wertvolle Instrumente zur Kommunikation und Interaktion mit Mitarbeitern, Kunden, Geschäftspartnern und anderen. UTC erkennt die Bedeutung des Datenschutzes für online erfasste Informationen an und hat eine spezielle Internet-Datenschutzrichtlinie (Internet Privacy Policy – „IPP“) zur Handhabung der auf seinen Websites erfassten personenbezogenen Mitarbeiterdaten erarbeitet. Wenn personenbezogene Mitarbeiterdaten aus dem EWR übermittelt werden, ist die IPP dieser Erklärung untergeordnet.

DURCHSETZUNG

UTC überprüft die Durchsetzung dieser Richtlinien in Form periodischer Audits und Umfragen unter Personalmanagern und anderen Mitarbeitern, die personenbezogene Mitarbeiterdaten handhaben. Damit wird die Einhaltung dieser Erklärung verifiziert und die Gewährung der jährlichen *Safe Harbor*-Erfüllungszertifizierungen durch das US Department of Commerce (US-Wirtschaftsministerium) erleichtert. Gegen Mitarbeiter, die dieser Erklärung zuwiderhandeln, werden Disziplinarmaßnahmen bis hin zur Kündigung verhängt.

KONTAKTINFORMATIONEN & SCHLICHTUNG VON STREITIGKEITEN

Fragen und Bedenken bzgl. dieser Erklärung und ihrer Umsetzung sind an den UTC Vice President, Business Practices, unter der nachstehenden Anschrift zu richten.

UTC untersucht gemäß den in dieser Erklärung enthaltenen Grundsätzen alle Fragen, Beschwerden und Streitigkeiten und versucht, diese zu lösen. Bei Beschwerden, die von UTC nicht gelöst werden können, nimmt UTC an den Schlichtungsverfahren des von europäischen Datenschutzbehörden gegründeten Gremiums zur Lösung von Streitigkeiten gemäß den *Grundsätzen des sicheren Hafens* teil. Gegebenenfalls leistet UTC den von dem Gremium verfügbaren spezifischen Maßnahmen Folge, um den *Grundsätzen des sicheren Hafens* zu genügen.

Fragen und Kommentare zu dieser Erklärung können dem UTC Vice President, Business Practices, per Post oder E-Mail wie folgt vorgelegt werden:

United Technologies Corporation
1 Financial Plaza Hartford,
Connecticut 06010
USA

Attention: Business Practices, Mail Stop 524-00
bpo@corphq.utc.com

ABÄNDERUNGEN DIESER ERKLÄRUNG

Diese Erklärung kann bei Bedarf von Zeit zu Zeit abgeändert oder ergänzt werden, um die *Grundsätze des sicheren Hafens* einzuhalten. Solche Abänderungen bzw. Ergänzungen werden in angemessener Weise öffentlich bekannt gemacht.