GRUNDSÄTZE DES „SICHEREN HAFENS“ ZUM DATENSCHUTZ

VORGELEGT VOM AMERIKANISCHEN HANDELSMINISTERIUM AM 21. JULI 2000

Die umfassende Rechtsvorschrift der Europäischen Union zum Schutz personenbezogener Daten, die Datenschutzrichtlinie (nachstehend „die Richtlinie“ genannt), trat am 25. Oktober 1998 in Kraft. Sie legt fest, dass personenbezogene Daten nur in Nicht-EU-Länder übermittelt werden können, die einen „angemessenen“ Schutz der Privatsphäre gewährleisten. Die Vereinigten Staaten und die Europäische Union haben beide das Ziel, den Datenschutz für ihre Staatsbürger zu verstärken, wobei die Vereinigten Staaten jedoch einen anderen Ansatz verfolgen als die Europäische Gemeinschaft. Die USA verwenden einen sektoralen Ansatz, der auf einer Mischung von Rechtsvorschriften, Verordnungen und Selbstregulierung basiert. Angesichts dieser Unterschiede fühlen sich viele US-Organisationen verunsichert bezüglich der Auswirkung des seitens der EU geforderten „Angemessenheits-Standards“ für die Übermittlung personenbezogener Daten aus der Europäischen Union in die Vereinigten Staaten.

Um diese Unsicherheit auszuräumen und einen berechenbareren Rahmen für solche Datenübermittlungen zu schaffen, legt das Handelsministerium unter seiner gesetzlichen Autorität, internationalen Handel zu pflegen, zu fördern und zu entwickeln, dieses Papier und sogenannte Häufig Gestellte Fragen - FAQs („die Grundsätze“) vor. Die Grundsätze wurden in Absprache mit der Industrie und der breiten Öffentlichkeit entwickelt, um den Handel zwischen der Europäischen Union und den Vereinigten Staaten zu erleichtern. Sie sind ausschließlich für den Gebrauch durch US-Organisationen bestimmt, die personenbezogene Daten aus der Europäischen Union erhalten, um sich für den „sicheren Hafen“ und die daraus erwachsende Vermutung der „Angemessenheit“ des Datenschutzes zu qualifizieren. Da die Grundsätze ausschließlich für diesen spezifischen Zweck erarbeitet wurden, können sie für andere Zwecke ungeeignet sein. Die Grundsätze können nicht benutzt werden als Ersatz für nationale Rechtsvorschriften über die Verarbeitung personenbezogener Daten in den Mitgliedstaaten, mit denen die Richtlinie umgesetzt wird.

Die Entscheidung der einzelnen Organisationen, sich für den „sicheren Hafen“ zu qualifizieren, ist vollkommen freiwillig, und die Organisationen können sich für das Konzept des „sicheren Hafens“ auf verschiedene Arten qualifizieren. Organisationen, die sich dazu entschließen, den Grundsätzen beizutreten, müssen die Grundsätze einhalten, um die Vorteile des „sicheren Hafens“ erhalten und behalten zu können, und sie müssen diese Absicht öffentlich bekanntmachen. Wenn sich eine Organisation beispielsweise einem vom Privatsektor

entwickelten Datenschutzprogramm anschließt, das sich an diese Grundsätze hält, qualifiziert sie sich für den „sicheren Hafen“. Darüber hinaus können sich Organisationen auch qualifizieren, wenn sie eigene Maßnahmen zum Schutz personenbezogener Daten entwickeln, sofern diese den Grundsätzen entsprechen. Verstößt eine Organisation, deren Datenschutzmaßnahmen ganz oder teilweise auf Selbstregulierung beruhen, gegen diese Selbstregulierung, muss dieser Verstoß auch gemäß Abschnitt 5 des Federal Trade Commission Act zur Verhinderung unlauterer und irreführender Praktiken oder ähnlichen Rechtsvorschriften verfolgbar sein (der Anhang enthält die Liste der von der EU anerkannten staatlichen Einrichtungen in den Vereinigten Staaten). Zudem können Organisationen, die Gesetzen, Regulierungs-, Verwaltungs- oder anderen Rechtsvorschriften (oder Regeln) unterliegen, die wirksam personenbezogene Daten schützen, ebenfalls in den Genuss der Vorteile des „sicheren Hafens“ gelangen. In allen Fällen gelten die Vorteile des Konzepts des „sicheren Hafens“ ab dem Tag, an dem die Organisation, die sich für die Grundsätze des sicheren Hafens qualifizieren möchte, gegenüber dem Handelsministerium (oder einer von ihm benannten Stelle) gemäß den in den FAQ zur Selbstzertifizierung dargelegten Leitlinien erklärt, dass sie den Grundsätzen beitritt.

Die Geltung dieser Grundsätze kann begrenzt werden (a) insoweit, als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss, (b) durch Gesetzesrecht, staatliche Regulierungsvorschriften oder Fallrecht, die unvereinbare Verpflichtungen oder ausdrückliche Ermächtigungen schaffen, vorausgesetzt, die Organisation kann in Wahrnehmung dieser Ermächtigungen nachweisen, dass die Nichteinhaltung der Grundsätze sich auf das Ausmaß beschränkte, das die Einhaltung übergeordneter berechtigter Interessen aufgrund eben dieser Ermächtigungen erforderte, oder c) wenn die Richtlinie oder das nationale Recht Ausnahmeregelungen vorsieht, sofern diese Ausnahmeregelungen unter vergleichbaren Voraussetzungen getroffen werden. Im Hinblick auf das Ziel eines wirksameren Schutzes der Privatsphäre sollen die Organisationen die Grundsätze in vollem Umfang und in transparenter Weise anwenden, unter anderem indem sie angeben, in welchen Fällen Abweichungen von den Grundsätzen, die nach b) zulässig sind, bei ihren Datenschutzmaßnahmen regelmäßig Anwendung finden werden. Aus demselben Grund wird, wenn die Wahlmöglichkeit nach den Grundsätzen und/oder nach dem US-Recht besteht, von den Organisationen erwartet, dass sie sich, sofern möglich, für das höhere Schutzniveau entscheiden.

Organisationen können aus praktischen oder anderen Gründen die Grundsätze auf alle Datenverarbeitungsverfahren anwenden, die Verpflichtung zur Anwendung der Grundsätze entsteht jedoch erst mit dem Beitritt zum „sicheren Hafen“. Bei manuell verarbeiteten Daten ist die Einhaltung der Grundsätze zur Qualifizierung für den „sicheren Hafen“ nicht erforderlich. Organisationen, die vom „sicheren Hafen“ profitieren wollen, um manuell verarbeitete Daten aus der EU zu erhalten, müssen die Grundsätze auf alle Daten anwenden, die nach ihrem Beitritt übermittelt werden. Eine Organisation, die die Vorteile des sicheren Hafens auf Personaldaten ausdehnen will, die im Rahmen eines Beschäftigungsverhältnisses aus der EU übermittelt werden, muss darauf hinweisen, wenn sie sich dem US-Handelsministerium (oder einer von diesem benannten Stelle) gegenüber auf die Grundsätze verpflichtet, und sie muss die in der

FAQ zur Selbstzertifizierung beschriebenen Anforderungen erfüllen. Organisationen können auch die in Artikel 26 der Richtlinie geforderten Garantien bieten, wenn sie in schriftlichen Vereinbarungen mit Stellen, die Daten aus der EU übermitteln, die Grundsätze für die materiellen Datenschutzvorschriften anwenden, sobald die weiteren Vorschriften für derartige Musterverträge von der Kommission und den Mitgliedstaaten genehmigt sind.

Für Fragen der Auslegung und der Einhaltung der Grundsätze des „sicheren Hafens“ (einschließlich der FAQ) und der einschlägigen Geschäftsbedingungen für den Datenschutz einzelner dem „sicheren Hafen“ angehörigen Organisationen gilt das US-Recht; es gilt nicht, wenn sich eine Organisation zur Zusammenarbeit mit europäischen Datenschutzbehörden verpflichtet hat. Sofern nicht anderweitig festgelegt, finden die Grundsätze des „sicheren Hafens“ in sämtlichen Teilen, einschließlich der FAQ, in allen Fällen, in denen sie relevant sind, Anwendung.

Personenbezogene Daten sind in beliebiger Form aufgezeichnete Daten über eine identifizierte oder identifizierbare Person, die unter die Richtlinie fallen und aus der Europäischen Union an eine US-Organisation übermittelt werden.

INFORMATIONSPFLICHT: Die Organisation muss Privatpersonen darüber informieren, zu welchem Zweck sie die Daten über sie erhebt und verwendet, wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, an welche Kategorien von Dritten die Daten weitergegeben werden und welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe der Daten einzuschränken. Diese Angaben sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen, wenn sie erstmalig gebeten werden, der Organisation personenbezogene Daten zu liefern, oder so bald wie möglich danach, auf jeden Fall aber bevor die Organisation die Daten zu anderen Zwecken verwendet als denen, für die sie von der übermittelnden Organisation ursprünglich erhoben oder verarbeitet wurden, oder bevor sie die Daten erstmalig an einen Dritten weitergibt.[1]

WAHLMÖGLICHKEIT: Die Organisation muss Privatpersonen die Möglichkeit geben zu wählen ("opt out"), ob ihre personenbezogenen Daten (a) an Dritte[1] weitergegeben werden sollen oder (b) für einen Zweck verwendet werden sollen, der mit dem ursprünglichen oder dem nachträglich von der betreffenden Person genehmigten Erhebungszweck unvereinbar ist. Der betroffenen Person muss die Ausübung ihres Wahlrechts durch leicht erkennbare und

[1] Die Übermittlung solcher Daten an einen Dritten ist nicht mitteilungspflichtig bzw. unterliegt nicht dem Grundsatz der Wahlmöglichkeit, wenn dieser im Auftrag oder auf Anweisung der Organisation tätig ist. Der Grundsatz der Weitergabe gilt jedoch auch in solchen Fällen.

verständliche, leicht zugängliche und kostengünstige Verfahren ermöglicht werden.

Bei sensiblen Daten (wie z. B. Angaben über den Gesundheitszustand, über Rassen- oder ethnische Zugehörigkeit, über politische, religiöse oder philosophische Überzeugungen, über die Mitgliedschaft in einer Gewerkschaft oder über das Sexualleben) benötigen die Organisationen die ausdrückliche Zustimmung („opt in“) der betroffenen Personen, wenn die Daten an Dritte weitergegeben oder für einen anderen als den ursprünglichen Erhebungszweck oder den Zweck verwendet werden sollen, dem die betroffene Person nachträglich durch Ausübung des Wahlrechts zugestimmt hat. In jedem Fall sollen die Organisationen alle ihnen von Dritten übermittelten Informationen als sensibel behandeln, die der Übermittler als sensibel einstuft und behandelt.

WEITERGABE: Eine Organisation darf Daten nur dann an Dritte weitergeben, wenn sie die Grundsätze der Informationspflicht und der Wahlmöglichkeit anwendet. Möchte eine Organisation Daten an einen Dritten weitergeben, der in ihrem Auftrag und auf ihre Anweisung tätig ist (vgl. Fußnote), kann sie dies tun, sofern der Dritte entweder dem „sicheren Hafen“ angehört oder der Richtlinie unterliegt, oder von einer anderen Feststellung angemessenen Schutzniveaus erfasst wird oder sich schriftlich in einer Vereinbarung mit der Organisation dazu verpflichtet, zumindest das Maß an Schutz personenbezogener Daten zu gewährleisten, das in den entsprechenden Grundsätzen des „sicheren Hafens" gefordert wird. Eine Organisation, die diese Forderungen erfüllt, kann nicht haftbar gemacht werden (sofern sie nichts anderes vereinbart hat), wenn ein Dritter, an den sie Daten übermittelt hat, Beschränkungen der Verarbeitung dieser Daten missachtet oder sie in einer Weise verarbeitet, die seinen Erklärungen widerspricht, es sei denn, die Organisation wusste oder konnte wissen, dass der Dritte die Daten in unzulässiger Weise verarbeiten würde, und hat keine angemessenen Schritte unternommen, um das zu unterbinden.

SICHERHEIT: Organisationen, die personenbezogene Daten erstellen, verwalten, verwenden oder verbreiten, müssen angemessene Sicherheitsvorkehrungen treffen, um sie vor Verlust, Mißbrauch und unbefugtem Zugriff, Weitergabe, Änderung und Zerstörung zu schützen.

DATENINTEGRITÄT: In Übereinstimmung mit den Grundsätzen müssen personenbezogene Daten für den beabsichtigten Verwendungszweck erheblich sein. Eine Organisation darf personenbezogene Daten nicht in einer Weise verarbeiten, die mit dem ursprünglichen Erhebungszweck oder mit dem Zweck unvereinbar ist, dem der Betroffene nachträglich zugestimmt hat. In dem für diese Zwecke notwendigen Umfang muss die Organisation durch angemessene Maßnahmen gewährleisten, dass die Daten für den vorgesehenen Zweck hinreichend zuverlässig, genau, vollständig und aktuell sind.

AUSKUNFTSRECHT: Privatpersonen müssen Zugang zu den personenbezogenen Daten haben, die eine Organisation über sie besitzt, und sie müssen die Möglichkeit haben, diese zu korrigieren, zu ändern oder zu löschen, wenn sie falsch sind, es sei denn, die Belastung oder die Kosten für die Gewährung des Zugangs würden in dem jeweiligen Fall in einem Mißverhältnis zu den Nachteilen für den Betroffenen stehen, oder Rechte anderer Personen als des Betroffenen würden verletzt.

DURCHSETZUNG: Für einen effektiven Schutz der Privatsphäre müssen Mechanismen geschaffen werden, die die Einhaltung der Grundsätze des sicheren Hafens gewährleisten, Rechtsbehelfe für Betroffene vorsehen, bei deren Daten die Grundsätze nicht eingehalten wurden, sowie Sanktionen für die Organisation, die die Grundsätze nicht befolgt. Diese Mechanismen müssen mindestens folgendes umfassen (a) leicht zugängliche, erschwingliche und von unabhängigen Stellen durchgeführte Verfahren, nach denen Beschwerden, die betroffene Personen unter Berufung auf die Grundsätze erhoben haben, behandelt werden und nach denen Schadensersatz geleistet wird, wenn das geltende Recht oder private Regelungen dies vorsehen; (b) Kontrollmaßnahmen, um zu überprüfen, ob die Bescheinigungen und Behauptungen der Unternahmen über ihre Datenschutzmaßnahmen der Wahrheit entsprechen und ob diese Maßnahmen wie angegeben durchgeführt werden; (c) Verpflichtungen zur Lösung von Problemen, die daraus resultieren, dass Organisationen die Einhaltung der Grundsätze zwar erklärt, sich aber trotzdem nicht daran gehalten haben, sowie entsprechende Sanktionen für diese Organisationen. Die Sanktionen müssen hinreichend streng sein, um sicherzustellen, dass die Organisationen die Grundsätze einhalten.