

## **GDPdU – Eine Maßnahme zur IT-Sicherheit**

Seit dem 01. Januar 2002 können Steuerprüfer auf steuerrelevante Unterlagen, die in einem Unternehmen in digitaler Form vorliegen, zugreifen. Die Anforderungen sind hierzu in den „GDPdU“ zusammengefasst, den „Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“. Viele Unternehmen stellen diese Anforderungen nach wie vor vor erhebliche Probleme. In Anbetracht der Tatsache, dass bereits erste gerichtliche Entscheidungen vorliegen, sollte jedes Unternehmen für sich die Frage klären, welche organisatorischen Anforderungen der elektronische Datenzugriff der Finanzverwaltung nach sich zieht.

### Rechtsgrundlagen

§ 147 Abs. 6 Abgabenordnung (AO) bildet die Ermächtigungsgrundlage für den elektronischen Datenzugriff der Finanzverwaltung. Sie sieht das Recht der Finanzbehörden vor, elektronisch gespeicherte Daten des Steuerpflichtigen einzusehen und für Prüfungszwecke auszuwerten. Elektronisch aufgezeichnete steuerrelevante Daten müssen während der gesetzlichen Aufbewahrungsfrist in maschinell auswertbarer Form vorgehalten werden (§ 147 Abs. 2 Nr. 2 AO). Diese Regelung korrespondiert mit den handelsrechtlichen Vorschriften. Buchführungs- und Jahresabschlussunterlagen und Buchungsbelege müssen 10 Jahre, sonstige steuerrelevante Unterlagen müssen 6 Jahre aufbewahrt werden (§ 147 Abs. 3 AO). Daneben stellt § 200 AO klar, dass ein Unternehmer zur Mitwirkung und Unterstützung bei Außenprüfungen verpflichtet ist. Auch im Handelsgesetzbuch sind Anforderungen hinsichtlich der Buchführung gesetzlich geregelt. Eine Buchführung muss so geschaffen sein, dass sich ein sachverständiger Dritter in angemessener Zeit einen Überblick verschaffen kann (§ 238 Abs. 1 HGB). Wird die Buchführung in einem EDV-System durchgeführt, sind die Grundsätze ordnungsgemäßer Buchführung zu beachten (§ 239 Abs. 4 HGB). Daneben sind beispielsweise Vorschriften aus dem Umsatzsteuergesetz zu beachten.

Seit dem 01.01.2002 ist die Finanzverwaltung berechtigt, elektronisch gespeicherte Daten des Steuerpflichtigen auszuwerten. Es wird eine jederzeitige Verfügbarkeit elektronisch gespeicherter Daten mit Bedeutung für die Besteuerung verlangt. Darüber hinaus müssen die Daten jederzeit lesbar gemacht werden können.

Das Bundesfinanzministerium hat mit Stand vom 01.02.2005 einen FAQ-Katalog veröffentlicht, der zum Datenzugriffsrecht der Finanzverwaltung Stellung nimmt. Die Informationen er-

läutern einige Zweifelsfragen des Datenzugriffs, sind aber nur eine Information des Steuerpflichtigen und nicht verbindlich.

### Möglichkeiten des Datenzugriffs

Der Prüfer kann im Rahmen einer Außenprüfung nach pflichtgemäßem Ermessen entscheiden, welche Art des Datenzugriffs er wählt. Einen „Online-Zugriff“ auf das betriebliche EDV-System ist ausdrücklich ausgeschlossen. Dem Prüfer stehen nur folgende Varianten des Datenzugriffs zur Verfügung:

- Unmittelbarer Datenzugriff,
- mittelbarer Datenzugriff,
- Datenträgerüberlassung.

Nach der Auffassung des Bundesfinanzministeriums beinhaltet der unmittelbare Datenzugriff den Nur-Lesezugriff auf die EDV-Systeme durch den Prüfer zur Prüfung der Buchhaltungsdaten, Stammdaten und Verknüpfungen. Der Prüfer darf auch vorhandene Auswertungsprogramme des betrieblichen EDV-Systems zwecks Filterung und Sortierung der steuerlich relevanten Daten nutzen.

Bei einem mittelbaren Datenzugriff müssen die steuerlich relevanten Daten nach den Vorgaben des Prüfers vom Unternehmen oder einem beauftragten Dritten maschinell ausgewertet werden. Anschließend kann dann ein Nur-Lesezugriff durchgeführt werden. Der Prüfer darf nur eine maschinelle Auswertung mit den im EDV-System vorhandenen Auswertungsmöglichkeiten verlangen. Die dabei entstehenden Kosten sind vom Unternehmen zu tragen. Darüber hinaus sind die Unternehmen zur Unterstützung des Prüfers durch Personen verpflichtet, die mit dem EDV-System vertraut sind.

Bei der Datenträgerüberlassung werden dem Prüfer in maschinell auswertbarer Form die notwendigen Informationen zur Verfügung gestellt.

Ein Prüfer ist nicht berechtigt, eigenmächtig Daten aus dem betrieblichen EDV-System herunterzuladen.

### Steuerlich relevante Daten

In der Praxis schwierig zu klären ist die Frage, welche Daten als steuerlich relevant einzustufen sind. In dem FAQ-Katalog der Finanzverwaltung wird entwaffnend ehrlich darauf hingewiesen, dass es zu diesem Terminus keine allgemein gültige Definition gibt. Nebulös umschreibt die Finanzverwaltung den Begriff steuerlich relevante Daten wie folgt:

„Steuerlich relevant“ sind Daten immer dann, wenn sie für die Besteuerung des Steuerpflichtigen von Bedeutung sein können.

Diese Definition und Beschreibung erklärt allerdings in der Praxis die Detailfragen nicht. An dieser Stelle ist der Steuerpflichtige mehrfach gefordert. Er muss zum einen die steuerrelevanten Daten von den anderen Daten abgrenzen. Darüber hinaus muss er auch organisatorisch sicherstellen, dass ein Zugriff nur auf die steuerrelevanten Daten möglich ist. Dabei sind datenschutzrechtliche oder besondere berufsspezifische Gesichtspunkte zu beachten. Bei Meinungsverschiedenheiten ist nach Auffassung des Bundesfinanzministeriums im Einzelfall zu entscheiden, welche Folgerungen zu ziehen sind. Auch dies lässt einen breiten Interpretationsspielraum offen.

### Risiken aus anwaltlicher Sicht

Die Umsetzung der GDPdU in der Praxis hat aus anwaltlicher Sicht verschiedene Risiken.

#### **Risiko 1**

Viele Unternehmen versuchen in der Praxis, nur das Thema elektronischer Datenzugriff in den Griff zu bekommen. Eine solche punktuelle Betrachtung wird den rechtlichen Anforderungen nicht gerecht. Wie eingangs gezeigt, gibt es beispielsweise hinsichtlich der Archivierungspflichten von E-Mails nicht nur steuerrechtliche, sondern auch handelsrechtliche Anforderungen. Daneben ist sowohl aus arbeitsrechtlichen als auch aus strafrechtlichen Aspekten eine Untersagung der privaten E-Mail- und Internet-Nutzung durch die Mitarbeiter im Unternehmen angezeigt. Weiterhin sind datenschutzrechtliche Gesetzesvorschriften zu beachten. Sinnvoll ist daher die Einbindung der GDPdU in ein Gesamtkonzept zur IT-Sicherheit.

## **Risiko 2**

Ein weiteres erhebliches Risiko stellt in der Praxis die Klärung der Frage dar, welche Daten steuerlich relevant sind. Es darf auf die obigen Ausführungen verwiesen werden. Die Verantwortung für die richtige Einordnung liegt beim Steuerpflichtigen.

## **Risiko 3**

Ein weiteres Risiko stellt ein Systemwechsel in der IT-Infrastruktur dar. Bei Migration ist sicherzustellen, dass die Anforderungen der GDPdU beachtet werden. Es darf nur das Format der Daten umgesetzt werden, eine inhaltliche Änderung der Daten ist nicht zulässig.

## **Risiko 4**

Bei der Übernahme eines Betriebes sind ebenfalls die Anforderungen der GDPdU zu beachten. Grundsätzlich hat die Übernahme eines Betriebes keinen Einfluss auf die Pflichten zur Aufbewahrung prüfungsrelevanter Daten. Der Erwerber muss diese Pflichten im Zuge der Gesamtrechtsnachfolge erfüllen. Insoweit sind entsprechende organisatorische und auch vertragliche Absicherungen gegenüber dem Unternehmensverkäufer zu treffen.

## Zusammenfassung

Der elektronische Datenzugriff ist nur ein Teilaspekt des großen Themas „IT-Sicherheit“. Es ist Unternehmen dringend zu empfehlen, diesbezüglich eine Gesamtkonzeption zu erstellen. Dabei ist auf die altbekannte Tatsache hinzuweisen, dass die Installation von Maßnahmen zur IT-Sicherheit Aufgabe der Unternehmensleitung ist. Wenn Geschäftsführer und Vorstände diesbezüglich ihre organisatorischen Pflichten vernachlässigen, so erhöht sich das Risiko einer persönlichen Haftung für eine solche Pflichtverletzung erheblich.