## HIM 41 Unterrichtungspflichten bei der Datenerhebung (nach § 4 Abs. 3 BDSG)

### 1. Informationspflicht

Das im Jahre 2001 auf Grund der EG Datenschutzrichtlinie novellierte BDSG hat den Grundsatz der Direkterhebung der Daten beim Betroffenen besonders betont und sieht hierzu bestimmte Unterrichtungs-, Hinweis- und Aufklärungspflichten bei der Datenerhebung vor. Der Betroffene soll dadurch in die Lage versetzt werden, darüber entscheiden zu können, ob er die Daten gegenüber der erhebenden Stelle bekannt geben will oder nicht. Diese Regelungen gelten für öffentliche wie für nichtöffentliche Stellen gleichermaßen. Von besonderer Bedeutung für den nichtöffentlichen Bereich ist § 4 Abs. 3 Satz 1 BDSG. Danach ist der Betroffene bei Erhebung der Daten von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,

2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und

3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,

zu unterrichten, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat.

Hinsichtlich der Identität der verantwortlichen Stelle sind der Name und die Anschrift anzugeben. Der Hinweis auf den Zweck der Erhebung soll den Betroffenen darüber unterrichten, wozu die Daten benötigt werden, soweit die Zweckbestimmung nicht offensichtlich ist. Es sind sämtliche Zwecke anzugeben. Deshalb ist, wenn die im Rahmen eines Vertragsverhältnisses mit dem Betroffenen verarbeiteten Daten auch für Werbezwecke verwendet werden sollen, auch dies anzugeben. Offenzulegen sind auch die Kategorien von Empfängern der Daten, zu denen im Einzelfall auch Stellen gehören können, die die Daten im Auftrag verarbeiten sollen.

Die Unterrichtungspflicht entfällt, wenn die betroffene Person von der Information, die sie erhalten soll, bereits auf andere Weise Kenntnis erlangt hat. Die verantwortliche

Stelle muss dies, wenn sie sich hierauf berufen will, allerdings nachweisen können. Nur hinsichtlich der Empfänger der Daten genügt es, dass der Betroffene nach den Umständen des Einzelfalles hiermit rechnen musste. Hierzu genügt es nicht, dass die Datenübermittlung (beispielsweise eine Bonitätsanfrage bei einer Auskunftei) oder sonstige Datenweitergabe „branchenüblich“ ist; erforderlich ist auch, dass dies den Betroffenen bekannt ist. Es empfiehlt sich daher, den Betroffenen im Zweifelsfall zu unterrichten.

## 2. Rechtsfolgen einer unterlassenen Unterrichtung

Zu der Frage, welche Rechtsfolgen die Nichtbeachtung der Unterrichtungspflicht nach sich zieht, enthält das BDSG keine spezielle Regelung, auch keinen Bußgeldtatbestand, der einen solchen Verstoß ausdrücklich sanktionieren würde. Zu berücksichtigen ist jedoch, dass die Informationspflicht in § 4 BDSG, der zentralen Vorschrift über die Zulässigkeit der Datenverarbeitung, verankert worden ist. Daraus wird teilweise der Schluss gezogen, dass § 4 Abs. 3 BDSG als Zulässigkeitstatbestand anzusehen ist mit der Konsequenz, dass die Nichtbeachtung der Informationspflichten stets zur Unzulässigkeit der Datenerhebung und damit auch zur Unzulässigkeit der weiteren Verarbeitung führt.

Schutzzweck der Regelung ist, wie eingangs ausgeführt, den Betroffenen in die Lage zu versetzen, darüber entscheiden zu können, ob er die Daten angeben will oder nicht. Ein Verstoß gegen die Unterrichtungspflichten nach § 4 Abs. 3 Satz 1 BDSG wirkt sich deshalb in denjenigen Fällen auf die Zulässigkeit aus, in denen durch die Nichtbeachtung der Informationspflichten der Grundsatz von Treu und Glauben verletzt wird. Ein Verstoß gegen Treu und Glauben ist bei der Zulässigkeitsprüfung (§§ 28 und 29 BDSG) zu berücksichtigen. Eine unzulässige Datenerhebung hat dabei zur Folge, dass die Daten nicht weiterverwendet (verarbeitet oder genutzt) werden dürfen und der Betroffene einen Anspruch auf Löschung der Daten hat (§ 35 Abs. 2 Nr. 1 BDSG). In diesem Fall liegt auch eine Ordnungswidrigkeit nach § 43 Abs. 2 Nr. 1 BDSG vor.

Ob ein Verstoß gegen die Unterrichtungspflicht zur Unzulässigkeit der Datenerhebung führt, ist für jeden Einzelfall gesondert zu prüfen. Beispielhaft sind folgende Fälle zu nennen:

* Ein Unternehmen hat Daten des Betroffenen im Rahmen eines Kaufvertrages erhoben. Es möchte nun diese Daten zum Zwecke der Werbung für andere eigene Produkte verwenden. Es handelt sich dabei um einen anderen Zweck als den ursprünglich bei der Datenerhebung beabsichtigten. Das Unternehmen muss nach § 4 Abs. 3 Satz 1 Nr. 2 BDSG auch auf diese Zweckbestimmung hinweisen. Es genügt nicht, dass der Betroffene bei der werblichen Ansprache nach § 28 Abs. 4 BDSG auf die Möglichkeit des Werbewiderspruchs hingewiesen wird.

* Beabsichtigt das Unternehmen, die personenbezogenen Daten des Betroffenen zu Werbezwecken anderer (Partner-) Unternehmen zu übermitteln oder für diesen Zweck zu nutzen, gilt dies erst recht. Mit einer solchen Datenübermittlung oder -nutzung muss der Betroffene zum Zeitpunkt des Abschlusses des Vertrages in der Regel nicht rechnen. Unterbleibt die Unterrichtung nach § 4 Abs. 3 Satz 1 BDSG, wird regelmäßig von der Unzulässigkeit der Datenverarbeitung auszugehen sein.

* Ein Unternehmen führt zur Gewinnung von Informationen für Zwecke der gezielten Werbung eine (schriftliche oder mündliche) Umfrage durch. Wird in diesem Fall nur von „Markt- und Meinungsforschung“ oder von der „Zusendung von Informationen“ gesprochen, ist dies keine zutreffende und klare Information über den Verwendungszweck, wenn in Wirklichkeit die Werbung für Produkte und Dienstleistungen einzelner Unternehmen beabsichtigt wird. Anzugeben ist auch, an welche Stellen die Daten übermittelt werden sollen (zum Beispiel Nahrungsmittelhersteller, Autohändler, Versicherungsunternehmen oder Verlage).

Es zeigt sich daher, dass ein Verstoß gegen § 4 Abs. 3 BDSG ein erhebliches rechtliches Risiko darstellt und nur die konsequente Beachtung der Informationspflicht nach § 4 Abs. 3 BDSG die Gewähr dafür bietet, dass die Erhebung und weitere Datenverarbeitung rechtmäßig ist.

## HIM 41 Einsatz biometrischer Verfahren beim Bezahlen im Handel und in der Gastronomie

### 1. „Bezahlen mit Fingerabdruck“

Neben der Barzahlung finden im Handel und in der Gastronomie zunehmend bargeldlose Zahlungsformen Anwendung. Beim bargeldlosen Bezahlen gewährt der Händler oder Gastronom dem Kunden einen Warenkredit, bis der Rechnungsbetrag auf seinem Konto gutgeschrieben ist. Oft wird für diese Zahlungsform das Lastschriftverfahren verwendet[1]. Seit kurzem werden beim Bezahlen mittels Lastschriftverfahren auch biometrische Verfahren eingesetzt, bei denen sich der Kunde über seinen Fingerabdruck identifiziert.

Hierzu lässt sich der Kunde zuerst beim Unternehmen registrieren. Dabei werden die zum Lastschrifteinzug erforderlichen Bestandsdaten des Kunden sowie ein sogenanntes Template eines Fingerabdrucks als Referenzdatum erhoben und in der Kundendatenbank gespeichert. Bei einem Template wird nicht der Fingerabdruck als Bild, sondern die Position relevanter Punkte der Fingerlinien mathematisch in eine Formel (Hashwert) umgewandelt und verschlüsselt gespeichert. Der Original-Fingerabdruck kann bei diesem Verfahren nicht reproduziert werden. Gleichzeitig ermächtigt der Kunde das Unternehmen zur Abbuchung zukünftiger offener Forderungen von seinem Girokonto.

Möchte der Kunde eine Rechnung bargeldlos bezahlen, so bestätigt er die Richtigkeit des Rechnungsbetrags durch Auflegen seines Fingers auf einen Fingerabdruckscanner und autorisiert das Unternehmen damit, den Rechnungsbetrag bei der Bank einzuziehen. Von dem Fingerabdruck wird ein neues, temporäres Template erzeugt und mit dem hinterlegten Referenztemplate verglichen. Besteht Übereinstimmung, so gilt die Identifizierung als erfolgt und der Abbuchungsauftrag wird an die Bank weitergegeben.

[1] Siehe auch Hinweis Nr. 37 vom 11.01.1999, Ziff. 3

## 2. Datensparsamkeit

Bei einem Fingerabdruck handelt es sich um ein personenbezogenes Datum im Sinne des § 3 Abs. 1 BDSG. Weitere personenbezogene Daten sind die Bestandsdaten der Kundendatenbank und die Daten über den Konsum oder die gekauften Waren des Kunden.

Dem Grundsatz der Datensparsamkeit wird dadurch Rechnung getragen, dass bei dem Verfahren der Fingerabdruck nicht als Bild, sondern als mathematischer Wert gespeichert wird, der aus der Lage bestimmter charakteristischen Punkten der Fingerlinien gebildet wird. Die Berechnung erfolgt mit einer „Einweg-Funktion“ (Hashwert), bei der es nicht möglich ist, das Bild des Fingerabdrucks zu rekonstruieren. In Verbindung mit einer Lebenderkennung, bei der immer nur ein Vergleich mit einem lebenden Finger, nicht mit dem Bild eines Fingerabdrucks möglich ist, ist es praktisch ausgeschlossen, dass die gespeicherten Fingerabdruck-Informationen für andere Zwecke genutzt werden können.

Aus Datenschutzgründen wäre zwar grundsätzlich eine sogenannte dezentrale Speicherung der Daten in verschlüsselter Form auf einer Chipkarte, die der Betroffene mit sich führt, zu bevorzugen. Bei einem Verfahren, das das Mitführen von EC- oder Kreditkarte entbehrlich machen soll, würde eine dezentrale Datenspeicherung auf einer vorzulegenden Chipkarte jedoch dem Sinn des Verfahrens widersprechen.

## 3. Einwilligung

Rechtsgrundlage für die Erhebung, Nutzung und Speicherung der personenbezogenen Daten ist die schriftliche Einwilligung des Kunden bei seiner Registrierung. Voraussetzung für die Wirksamkeit der Einwilligung ist eine umfassende Information, nicht nur über das Lastschriftverfahren, sondern auch über Art und Umfang der Verarbeitung der Fingerabdruckdaten.

Der Kunde muss zumindest darüber informiert werden,

- dass ein charakteristisches Muster seiner Fingerlinien als Template gespeichert wird,
- dass diese Daten bei jedem Bezahlvorgang zum Vergleich und zur Bestätigung seiner Identität herangezogen werden,
- dass dies der einzige Anwendungszweck der biometrischen Daten ist,
- dass er selbst jederzeit die Löschung seiner personenbezogenen Daten verlangen kann und
- wann eine automatische Löschung seiner Daten erfolgt, wenn die Bezahlmöglichkeit längere Zeit nicht mehr genutzt wird.

**4. Technische und organisatorische Maßnahmen**

Die Einwilligung ermächtigt lediglich dazu, die Fingerabdruckdaten bei der jeweils verantwortlichen Stelle (dem Handels- oder Gastronomiebetrieb) zum Zwecke der Abrechnung im Lastschriftverfahren zu verarbeiten. Ausgeschlossen ist daher, die Daten weiterzugeben und beispielsweise in einer übergeordneten Datenbank zusammenzuführen. Um zu verhindern, dass die Templates verschiedener Anwender eines Verfahrens miteinander verknüpft werden können, muss der Algorithmus der Hashwertbildung bei der Templateerzeugung zwischen den Unternehmen, die das Verfahren eines Systemanbieters anwenden, variieren, so dass der Fingerabdruck desselben Fingers bei unterschiedlichen Anwendern auch zu unterschiedlichen Templates führt.

Ferner ist sicherzustellen, dass keine unberechtigten Zugriffe auf die im Unternehmen gespeicherten Templates durchgeführt werden können. Dieses kann am besten durch die verschlüsselte Speicherung der Kundendatenbank auf einem Rechnersystem ohne Zugang zu öffentlichen Netzen gewährleistet werden.

## HIM 41 Verarbeitung von IP-Adressen durch Inhaltsanbieter im Internet

Die Aufsichtsbehörde hat eine Anzahl von Tele- und Mediendiensten (Versandhäuser, Verlage und andere sogenannte Internet-Inhaltsanbieter; nachfolgend als Inhaltsanbieter benannt) datenschutzrechtlich geprüft. Nicht in die Prüfung einbezogen wurden Internet-Zugangsanbieter (nachfolgend als Zugangsanbieter bezeichnet), die ausschließlich den Zugang des Nutzers zum Internet bereitstellen. Bei der Prüfung der Inhaltsanbieter wurde festgestellt, dass die Verarbeitung von IP-Adressen (IP = Internet Protokoll) unterschiedlich gehandhabt wird.

Nimmt der Nutzer einen Tele- oder Mediendienst in Anspruch, so fallen als Daten aus dem Nutzungsvorgang insbesondere technische Daten wie IP-Adresse, System- und Browserdaten an. Diese Daten werden vom Inhaltsanbieter benötigt, um den Dienst durchführen und die angebotene Funktionalität gewährleisten zu können. Das wichtigste Nutzungsdatum ist dabei die IP-Adresse. Die IP-Adressen dienen der Übertragung der Daten zwischen dem Absender und dem Empfänger, das heißt der Weitervermittlung der zu übertragenden Datenpakete und der Wegewahl (Routing) über das Internet. Hierzu hat jeder Rechner im Internet eine eindeutige IP-Adresse, die vom Zugangsanbieter bei jeder Einwahl in das Internet für jede Sitzung neu zugeteilt wird. Man spricht hierbei von einer dynamischen Vergabe von IP-Adressen (sogenannte dynamische IP-Adressierung).

Bei der Überprüfung der Inhaltsanbieter stellte sich heraus, dass die IP-Adresse über das Ende des Nutzungsvorgangs hinaus

- zur Gewährleistung der Datensicherheit sowie
- zum Schutz vor Zahlungsausfällen

gespeichert wurde.

Diese genannten Zwecke sind für die verschiedenen Gruppen von Inhaltsanbietern von unterschiedlicher Bedeutung:

**1. Fallgruppe:**

Der Nutzer kann sich die Inhalte der Internet-Seiten anschauen und Informationen ausdrucken beziehungsweise kostenlos herunterladen. Der Inhaltsanbieter erhebt jedoch keine zusätzlichen personenbezogenen Daten (auch keine E-Mail-Adresse). Eine Zusammenführung mit den personenbezogenen Daten des Nutzers, wie sie beim Zugangsanbieter vorhanden sind, ist rechtlich und praktisch ausgeschlossen. Die IP-Adresse ist in diesem Fall für den Inhaltsanbieter kein personenbezogenes Datum. Die Datenschutzvorschriften des Teledienstedatenschutzgesetzes (TDDSG) beziehungsweise des Mediendienstestaatsvertrages (MDStV) finden somit hinsichtlich der Erhebung und der weiteren Verarbeitung der IP-Adresse durch den Inhaltsanbieter keine Anwendung.

**2. Fallgruppe:**

Der Nutzer führt im Verlauf der Sitzung Bestellungen durch oder gibt seine E-Mail-Adresse für die Zusendung von Informationen an. Die IP-Adresse wird durch die Eingabe der Nutzerdaten für den Inhaltsanbieter personenbeziehbar. Die Datenschutzvorschriften des Teledienstedatenschutzgesetzes (TDDSG) beziehungsweise des Mediendienstestaatsvertrages (MDStV) sind somit hinsichtlich der Erhebung und weiteren Verarbeitung der IP-Adresse durch den Inhaltsanbieter anzuwenden.

**3. Fallgruppe:**

Der Nutzer ist dem Inhaltsanbieter schon bekannt und meldet sich über Name, User-ID oder Kundennummer zur Nutzung des Dienstes an. Die gespeicherte IP-Adresse ist als ein personenbeziehbares Datum zu sehen. Die entsprechenden Datenschutzvorschriften sind demzufolge auch hier anzuwenden.

Grundsätzlich darf der Inhaltsanbieter nach § 6 Abs. 1 TDDSG beziehungsweise § 19 Abs. 2 MDStV personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erheben, verarbeiten oder nutzen, soweit dies erforderlich ist, um die Inanspruchnahme von Telediensten bzw. Mediendiensten zu ermöglichen und abzurech-

nen (Nutzungsdaten). Über das Ende des Nutzungsvorgangs hinaus dürfen Nutzungsdaten jedoch verarbeitet und genutzt werden,

- soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind (§ 6 Abs. 4 TDDSG beziehungsweise § 19 Abs. 5 MDStV) oder
- wenn zu dokumentierende tatsächliche Anhaltspunkte auf Entgeltverkürzung vorliegen (§ 6 Abs. 8 TDDSG beziehungsweise § 19 Abs. 9 MDStV).

Zu den von den Inhaltsanbietern genannten Speicherzwecken wie der Gewährleistung der Datensicherheit und dem Schutz vor Zahlungsausfällen haben wir folgende Haltung eingenommen:

## 1 Gewährleistung der Datensicherheit

Durch die Protokollierung des Nutzerverhaltens über einen gewissen Zeitraum hinweg ist es möglich, bis dahin unbemerktes Eindringen zu entdecken und die Eindringmethoden zu analysieren. Im Falle eines strafbaren Eindringens kann die betreffende IP-Adresse an die Strafverfolgungsbehörden weitergegeben werden.

### *1.1 Anzuwendende Vorschriften*

Technische und organisatorische Vorkehrungen sind dem Inhaltsanbieter zum einen nach § 4 Abs. 4 TDDSG vorgeschrieben. Diese Vorschrift ist jedoch nicht abschließend, da sie sich nur auf einzelne, teledienstspezifische Anforderungen bezieht. Daher findet § 9 BDSG nach § 1 Abs. 2 TDDSG ergänzende Anwendung. Von der ergänzenden Anwendung der allgemeinen Vorschriften des BDSG geht der Bundesgesetzgeber in anderem Zusammenhang ebenfalls aus, wie die Aufhebung des § 3 Abs. 4 TDDSG (Grundsätze zur Datenvermeidung und -sparsamkeit) im Zuge der Novellierung des TDDSG im Jahre 2001 gezeigt hat. Zur Begründung führte der Gesetzgeber aus, dass diese Regelung mit der Novellierung des Bundesdatenschutzgesetzes unter § 3a Satz 1 BDSG als übergreifende Regelung übernommen wurde und es daher einer besonderen Regelung im TDDSG nicht mehr bedarf. Maßgebli-

che Vorschriften nach § 9 BDSG und der Anlage hierzu sind im vorliegenden Fall Nr. 2 (Zugangskontrolle), Nr. 3 (Zugriffskontrolle), Nr. 4 (Weitergabekontrolle), Nr. 5 (Eingabekontrolle) und Nr. 7 (Verfügbarkeitskontrolle).

### *1.2 Datensicherheitskonzept*

Bei den Überprüfungen der Aufsichtsbehörde hat sich gezeigt, dass eine Reihe von Inhaltsanbietern die IP-Adressen systematisch und für einen längeren Zeitraum speicherten, ohne zuvor festgelegt zu haben, auf welche Weise und ob überhaupt in ihrem Fall eine Auswertung der Protokolldateien vorgenommen werden sollte. Offenbar hatten sie die Voreinstellungen des eingesetzten Programms übernommen.

Eine derartige Vorratsspeicherung ist nicht zulässig. Die Speicherung von IP-Adressen setzt voraus, dass die verantwortliche Stelle auf der Grundlage einer Bedrohungsanalyse ein konkretes Konzept entwickelt, auf welche Weise sie durch Speicherung und Auswertung der IP-Adressen die Datensicherheit gewährleisten will. Nur an Hand eines solchen Konzepts kann bestimmt werden, ob eine Speicherung erforderlich ist und in welchem Umfang und für welche Dauer dies der Fall ist.

In diesem Konzept ist auch vorzusehen, dass die Wirksamkeit der getroffenen Schutzmaßnahmen überprüft wird (das heißt kontrolliert wird, ob Unbefugte zugegriffen haben), und welche Methoden und Verfahren der Ursachenanalyse zur Anwendung kommen.

### *1.3 Dauer der Speicherung der IP-Adressen*

Die Dauer der Speicherung von Nutzungsdaten im Rahmen der technischen und organisatorischen Maßnahmen nach § 9 BDSG muss sich aber an der Erforderlichkeit des konkreten Zweckes orientieren, das heißt, die Daten dürfen nur solange gespeichert werden, wie dies nach dem Konzept erforderlich ist, um die notwendigen Auswertungen und Analysen vorzunehmen. Es ist davon auszugehen, dass eine Speicherdauer der IP-Adressen von höchstens vier Wochen zur Gewährleistung der Datensicherheit ausreichend ist. Innerhalb dieses Zeitraums dürfte eine Auswertung

möglich sein, auch hinsichtlich der Erkennung von Eindringversuchen, die zeitlich versetzt aktiv werden, wie dies beispielsweise bei Trojanern der Fall sein könnte.

### *1.4 Informationspflicht*

Des weiteren hat der Inhaltsanbieter den Nutzer über die Verarbeitung seiner personenbezogenen Daten bereits zu Beginn des Nutzungsvorgangs umfassend zu unterrichten (§ 4 Abs. 1 TDDSG beziehungsweise § 18 Abs. 1 MDStV). Daher muss der Nutzer auch auf die Tatsache der Speicherung der IP-Adresse zur Gewährleistung der Datensicherheit und auf die vorgesehene Dauer der Speicherung hingewiesen werden. Wird ein Nutzer entgegen § 4 Abs. 1 TDDSG bzw. § 18 Abs. 1 MDStV nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet, handelt der Inhaltsanbieter nach § 9 Abs. 1 Nr. 2 TDDSG beziehungsweise § 24 Abs. 1 Nr. 5 MDStV ordnungswidrig.

### *1.5 Zweckbindung*

Die zur Gewährleistung der Datensicherheit gespeicherten Daten dürfen nach § 31 BDSG nur für diesen Zweck verarbeitet werden. Dies schließt allerdings nicht aus, die Protokolldaten aus dem Nutzungsvorgang zum Nachweis im Rahmen der Rechtsverfolgung gegen diejenigen Personen zu verwenden, die als Täter des unbefugten Zugriffs auf gespeicherte personenbezogene Daten ermittelt wurden.

## 2 Schutz vor Zahlungsausfällen

Bei kostenpflichtigen Diensten eines Inhaltsanbieters ist die Speicherung der IP-Adresse über das Ende des Nutzungsvorgangs hinaus im Rahmen der Abrechnung des Dienstes (kostenpflichtiger Seitenaufruf) zum Nachweis der Inanspruchnahme dieses Dienstes grundsätzlich zulässig, soweit und so lange dies hierfür erforderlich ist (§§ 6 Abs. 4 TDDSG beziehungsweise. 19 Abs. 5 MDStV).

Die IP-Adresse kann aber auch einen Ermittlungsansatz bieten, wenn bei der Bestellung von Waren oder Dienstleistungen falsche Angaben gemacht wurden. Mit Hilfe

der IP-Adresse kann der Verantwortliche von der Strafverfolgungsbehörde über den Zugangsanbieter ermittelt werden, damit der Inhaltsanbieter ggf. seine zivilrechtlichen Ansprüche aus der Bestellung und Lieferung durchsetzen kann. Da es sich bei falschen Angaben im Bestellformular nicht um den Fall des unberechtigten Zugriffs auf gespeicherte personenbezogene Daten handelt, der unter Überwindung der technisch-organisatorischen Datensicherheitsmaßnahmen erfolgt, kann die Speicherung und Nutzung der IP-Adresse nicht mit dem Gesichtspunkt der Gewährleistung der Datensicherheit gerechtfertigt werden. Sie ist daher nur auf der Grundlage einer (elektronischen) Einwilligung des Nutzers nach § 4 Abs. 2 TDDSG beziehungsweise § 18 Abs. 2 MDStV zulässig.

## HIM 41 Digitale Fotokopierer mit eigenen Speichermedien

Digitale Fotokopierer haben oftmals eine eingebaute Festplatte für die Zwischenspeicherung der Kopien vor dem Ausdruck. Nicht immer wird darauf geachtet, dass der Inhalt der Festplatte nach dem Abschluss des Druckvorgangs auch gelöscht wird.

Insoweit ist zwar fraglich, ob das BDSG im Hinblick auf § 1 Abs. 2 Nr. 3 Anwendung findet, da beim Anfertigen einer Fotokopie eines Dokuments mit personenbezogen Daten nur ein „Bild“ dupliziert wird und daher nicht von einer „Verarbeitung“ personenbezogener Daten unter Einsatz von „Datenverarbeitungsanlagen“ gesprochen werden kann. Nach § 27 Abs. 2 BDSG gelten die Vorschriften des Dritten Abschnitts des BDSG jedoch auch für personenbezogene Daten, die offensichtlich aus einer automatisierten Verarbeitung entnommen worden sind. Das bedeutet im Falle einer Fotokopie, dass das BDSG anwendbar ist, wenn das zu kopierende Dokument unmittelbar aus einer automatisierten Verarbeitung stammt (zum Beispiel Ausdruck einer Auswertung personenbezogener Daten).

Beim Einsatz eines digitalen Fotokopierers mit eingebauter Festplatte findet § 9 BDSG (technische und organisatorische Maßnahmen) Anwendung, insbesondere Nr. 4 der Anlage zu § 9 BDSG (Weitergabekontrolle). Im Hinblick auf die Einschaltung eines (externen) Kundendienstmitarbeiters ist deshalb darauf zu achten, dass die auf der Festplatte zwischengespeicherten Daten nach Abschluss des Kopiervorgangs möglichst automatisch gelöscht werden oder eine Löschfunktion aktiviert wird. Ist insbesondere im Falle einer Störung nicht auszuschließen, dass noch Daten gespeichert sind, ist es erforderlich, die Wartungsfirma zu verpflichten, die Festplatte nach einem Ausbau und vor einer eventuellen Weiterverwendung bei Dritten zu löschen.