Ein Verbraucherdatenschutzinteressen im Firmennamen hervorhebendes Angebot warb mit seinem Service auch im Internet. Wahrheitswidrig wurde behauptet, unter anderem mit der Bundesnetzagentur zu kooperieren. Zudem verfügte die Firma offenbar in mehreren Fällen über die Bank- und Kontodaten der angerufenen Personen, wodurch diese verunsichert und zu einem Vertragsabschluss verleitet werden sollten. Die Nachforschungen haben ergeben, dass es sich bei dem angeblichen Firmensitz nur um eine Postadresse gehandelt hat. Tatsächlich befindet sich der Firmensitz in einem nicht der Europäischen Union angehörigen osteuropäischen Staat.

Ungeachtet des Umstands, dass sich Rechtshilfeersuchen der Strafverfolgungsbehörden an Nicht-EU-Staaten als durchweg schwierig erweisen, konnte im vorliegenden Fall als Erfolg verbucht werden, dass das Unternehmen ebenso wie auch andere vergleichbar in Erscheinung getretene Firmen ihre Aktivitäten und Geschäftsgebaren aufgrund der Warnhinweise der Datenschutzaufsichtsbehörden und Verbraucherschutzorganisationen eingestellt haben. Ob das "Geschäftsmodell" der Pseudodatenschutzangebote ausgelaufen ist, bleibt abzuwarten.

- Datenschutzaufsichtsbehörden, Verbraucherschutzorganisationen sowie die Bundesnetzagentur kooperieren nicht mit Diensten, die Daten von Bürgerinnen und Bürgern gegen Gebühr schützen wollen. Bei derartigen Angeboten ist Vorsicht geboten.

6.6 Untergeschobene Verträge am Telefon

Daten werden oft unberechtigt verwendet, um Betroffenen am Telefon vorzutäuschen, sie würden bereits seit längerem an Gewinnspielen teilnehmen. Solche Gespräche münden oft in ein Angebot zu einer Vertragsverlängerung oder enden mit der Erklärung, im Falle der Kündigung sei eine Gebühr zu entrichten.

Bei den Anrufen, die meist im großen Stil über Call-Center erfolgen, stehen rechtswidrig erlangte Bankkontodaten der Angerufenen im Fokus. Diese werden – etwa im Zusammenhang mit telefonischen Verkaufsanbahnungsgesprächen oder vermeintlichen Gewinnmitteilungen

– immer wieder zu unberechtigten Abbuchungen mittels Lastschrifteinzug bei Betroffenen genutzt.

Nach einer anderen, nicht minder betrügerischen Methode werden Betroffene am Telefon gezielt falsch informiert und zu einem Vertragsabschluss verleitet, oder aber ein Vertrag wird schlicht untergeschoben. Bei der inzwischen weit verbreiteten sogenannten Kündigungsmasche wird Betroffenen zum Beispiel erklärt, sie hätten bisher an einem – meist kostenlosen – Gewinnspiel teilgenommen. Solle der angebliche Vertrag nicht gebührenpflichtig weiterlaufen, bestehe nur die Möglichkeit einer Kündigung mit einer Frist von drei Monaten. Als "Gebühr" müssten dann drei Monatsbeiträge erhoben werden. Auf diese Weise erlangten betrügerische Anrufer im gesamten Bundesgebiet mehrere Millionen Euro. Betroffene wurden auf in diesen Fällen noch nicht abgeschlossene staatsanwaltschaftliche Ermittlungen hingewiesen.

Beweispflichtig auch für einen telefonisch abgeschlossenen Vertrag ist immer, wer diesen behauptet. Das Fehlen eines Vertrages kann auch einem eingeschalteten Inkassounternehmen entgegengehalten werden. Unabhängig hiervon können Betroffene Auskunftsansprüche unter anderem über die zu ihrer Person gespeicherten Daten und deren Herkunft geltend machen (§ 34 Bundesdatenschutzgesetz).

- Hier ist Vorsicht geboten. Wer sicher ist, dass kein Vertrag geschlossen wurde, sollte auch keine Zahlungen leisten oder einem unberechtigten Lastschrifteinzug widersprechen.

6.7 Bewertungsportale – Beurteilung in jeder Lebenslage

Die Bandbreite der Bewertungsportale im Internet hat in den letzten Jahren stark zugenommen. Die Bewertungsmöglichkeiten beschränkten sich früher vor allem auf Produkte, um die Kaufentscheidung anderer potentieller Käuferinnen und Käufer zu erleichtern. In letzter Zeit erstrecken sie sich jedoch auch auf Personen.

Zunächst bewegten sich die personenbezogenen Bewertungen in beruflichen Bereichen. So wurden beispielsweise Lehrerinnen und Lehrer, Handwerkerinnen und Handwerker sowie Ärztinnen und Ärzte bewer-

tet. Der Bundesgerichtshof hat im Fall des Bewertungsportals für Lehrerinnen und Lehrer "spickmich.de" entschieden, dass die Meinungsfreiheit das Persönlichkeitsrecht der Bewerteten überwiegt, sofern sich die Bewertungen auf die konkrete Berufsausübung beziehen. Da die berufliche Tätigkeit in der sogenannten Sozialsphäre erfolge, sei das Persönlichkeitsrecht der einzelnen Person bereits dadurch beschränkt, dass sie ihre Persönlichkeit innerhalb der sozialen Gemeinschaft entfalte. Jedoch hat das Gericht auch klargestellt, dass dem Persönlichkeitsrecht Vorrang einzuräumen ist, sobald die Äußerungen zu einer Stigmatisierung, sozialen Ausgrenzung oder Prangerwirkung führen können.

Im Rahmen der Aufsichtspraxis musste ich eine besorgniserregende Entwicklung feststellen. Es wurden nicht mehr nur Personen in Ausübung ihrer beruflichen Tätigkeit bewertet, sondern mittels eines "Single-Bewertungsportals" auch innerhalb ihres Privat- und Intimlebens. Singles konnten mit dessen Hilfe ihre "Internet-Flirtpartner" bewerten, die sie im realen Leben getroffen hatten.

Bewertet werden konnten unter anderem das Erscheinungsbild, das Auftreten, das Kommunikationsverhalten und die "Kusstechnik" der Flirtpartnerin oder des Flirtpartners. Darüber hinaus konnte angeklickt werden, ob es zum Geschlechtsverkehr gekommen war. Zusätzlich gab es ein moderiertes Freitextfeld, in dem die bewertende Person eintragen konnte, was ihr wichtig erschien. Diese Funktion bot die Gefahr, dass Kommentare mit beleidigendem Charakter oder gar intime Details veröffentlicht wurden.

Entgegen den gesetzlichen Erfordernissen wurde weder die Einwilligung der Bewerteten eingeholt noch ist eine nachträgliche Benachrichtigung erfolgt. Daher kannte die betroffene Person die Bewertung regelmäßig überhaupt nicht.

Die Bewertungen bedeuteten einen erheblichen Eingriff in die Intim- und Privatsphäre der Betroffenen, weil Werturteile hinsichtlich des Erscheinungsbildes, des Kommunikations- und Sexualverhaltens geäußert wurden. Ferner bestand durch den Umstand, dass das erteilte "Date-Zeugnis" weltweit im Internet eingesehen werden konnte, für Betroffene die Gefahr der sozialen Ausgrenzung und der Prangerwirkung. Dadurch wurde derart tief in die Rechte der Betroffenen eingegriffen, dass die Äußerungen offensichtlich nicht durch die Meinungsfreiheit gerechtfertigt werden konnten.

Nach der Kontaktaufnahme mit dem Unternehmen, das die Seite anbot, wurde das Bewertungsportal für mehrere Monate eingestellt. Seit kurzem ist es allerdings in abgewandelter Form wieder verfügbar. Sollte hier eine datenschutzgerechte Umsetzung nicht erfolgen, werde ich die notwendigen mir nach dem Gesetz möglichen Maßnahmen ergreifen.

Positiv davon hebt sich ein Portal ab, bei dem Patientinnen und Patienten unter einem Pseudonym Bewertungen über ihre behandelnden Ärztinnen und Ärzte abgeben können. Hierbei wird das Persönlichkeitsrecht der betroffenen Ärztinnen und Ärzte in höherem Maße als bei anderen Bewertungsportalen geschützt und zwar insbesondere durch

- objektivierbare und sachliche Bewertungskriterien, die weniger auf die persönlichen Eigenschaften der Ärztin oder des Arztes als auf generelle Aussagen über die Praxis abzielen,
- die Möglichkeit der Ärztinnen und Ärzte, Bewertungen zu kommentieren oder sich von der Bewertung ausnehmen zu lassen,
- den Ausschluss von Mehrfachbewertungen und den Verzicht auf Freitextfelder.

Dennoch bestehen auch hier Risiken, die zu einer Beeinträchtigung der Rechte der beteiligten Personen führen können. Beispielsweise ist nicht gewährleistet, dass die eine Bewertung abgebende Person tatsächlich bei der betroffenen Ärztin oder dem betroffenen Arzt in Behandlung gewesen ist. So ist auch nicht auszuschließen, dass Ärztinnen oder Ärzte selbst oder deren Beschäftigte oder Angehörige die Bewertung abgeben.

➡ Insgesamt halte ich die neuere Entwicklung der Bewertungsportale für bedenklich. Häufig werden der Schutz der einzelnen Person und die Gewährleistung ihres Rechts auf informationelle Selbstbestimmung nicht ausreichend berücksichtigt. Es ist daher dringend geboten, dass Stellen, die Bewertungsportale betreiben, ihren diesbezüglichen Verpflichtungen besser nach-

kommen und die datenschutzrechtlichen Vorschriften strikt einhalten.

6.8 Informationspflichten bei Datenpannen

Als Reaktion auf eine Vielzahl von Datenschutzskandalen in der jüngeren Vergangenheit wurde eine Informationspflicht bei Datenpannen in das Bundesdatenschutzgesetz (BDSG) aufgenommen. Nach dem Gesetz muss ein Unternehmen sowohl die Betroffenen als auch die zuständige Aufsichtsbehörde für den Datenschutz informieren, wenn sich bei ihm bestimmte, als besonders kritisch eingestufte Datenverluste ereignen. Die Informationspflicht besteht unabhängig davon, ob das Unternehmen den Datenverlust verschuldet hat.

Die bisher eingegangenen Meldungen über Datenpannen lassen erkennen, dass in konkreten Fällen noch eine große Unsicherheit bei den Unternehmen besteht, ob sie der Informationspflicht gemäß § 42a BDSG nachkommen müssen. Das Gesetz eröffnet hier einige Interpretationsspielräume, zu denen ich den anfragenden Unternehmen Hilfestellungen gegeben habe.

Beispielsweise sieht das Gesetz eine Meldepflicht nur in den Fällen vor, in denen schwerwiegende Beeinträchtigungen der Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Diese Einschränkung im Gesetzestext ist insofern überraschend, als die Datenkategorien, die eine Meldepflicht auslösen, ohnehin besonders schützenswert sind. Meldepflichtig sind Verluste personenbezogener Daten der folgenden Kategorien:

- Besondere Arten personenbezogener Daten gemäß § 3 Abs. 9 BDSG, wie etwa Gesundheitsdaten, Daten über eine politische oder religiöse Überzeugung oder über das Sexualleben,
- Daten, die einem Berufsgeheimnis unterliegen,
- Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen,
- Bank- und Kreditkartendaten.

Sofern personenbezogene Daten dieser genannten Kategorien unrechtmäßig an Dritte gelangen, ist eine schwerwiegende Beeinträchtigung der Betroffeneninteressen eigentlich der Regelfall. Unternehmen sollten bei einem solchen Datenverlust also grundsätzlich davon ausgehen, dass sie meldepflichtig sind. Praktisch müsste das Unternehmen besondere Gründe nennen können, warum im Einzelfall keine schwerwiegende Beeinträchtigung der Betroffeneninteressen vorliegt, wenn es die Information gemäß § 42a BDSG unterlässt.

Von den bisher gemeldeten Fällen stellen Diebstahl bzw. der Verlust von Hardware (PC, Laptop, Netbook, USB-Stick, externe Festplatte) einen signifikant hohen Anteil dar. Hier stehen die Unternehmen regelmäßig vor der Frage, ob schon der Verlust der Hardware bedeutet, dass eine dritte Stelle oder Person unrechtmäßig Kenntnis von den Daten erlangt hat, denn nur in diesem Fall entsteht die Pflicht zur Information nach § 42a BDSG. In aller Regel wissen die Unternehmen aber nicht, ob von Dritten auf die Daten zugegriffen wurde, wenn etwa ein Firmen-Laptop oder ein USB-Stick von einer Mitarbeiterin oder einem Mitarbeiter im Taxi liegen gelassen und nicht wieder aufgefunden wurde. Die Unternehmen können einen unberechtigten Zugriff jedenfalls dann nicht ausschließen, wenn die Daten nicht hinreichend verschlüsselt auf den Medien gespeichert waren. Bei Verlusten unverschlüsselter Daten, kann dem Gefahren abwehrenden Ziel des § 42a BDSG nur durch eine Information der Betroffenen in diesen Fällen angemessen Rechnung getragen werden.

Manche Unternehmen meldeten die Datenpannen vorsorglich zunächst nur meiner Behörde, informierten die Personen aber nicht, deren Daten verloren gingen. Dort wo Zweifel daran bestehen, ob überhaupt eine Informationspflicht nach § 42a BDSG entstanden ist, ist das grundsätzlich sachgerecht. Ist aber die Informationspflicht nach § 42a BDSG eindeutig, muss zeitgleich zur Meldung bei meiner Behörde eine Information der von dem Datenverlust betroffenen Personen erfolgen. Nur so kann die Gefahrenprävention in Missbrauchsfällen effektiv sein. Nur wenn eine Sicherung der Daten oder eine Strafverfolgung durch die zeitnahe Information der Betroffenen gefährdet wäre, ist eine Zeitverzögerung akzeptabel. Es sind also etwa Lücken in einem Firmensystem zunächst technisch zu schließen, bevor der Verlust von Daten über diese Lücke publik gemacht wird.