Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
www.datenschutzzentrum.de/
25.08.2008

Schlussfolgerungen aus dem Bekanntwerden des illegalen Verkaufs von Kontodaten

I. Der aktuelle Sachverhalt

Am 11. August wurde bekannt, dass ein früherer Mitarbeiter eines Callcenters in Lübeck der Verbraucherzentrale Schleswig-Holstein (VZ SH) eine Compact Disc (CD) übergeben hat, auf der mehr als 17.000 Datensätze mit Angaben zu Name, Adresse, Geburtsdatum und vollständiger Kontoverbindung enthalten sind, die zumindest teilweise von der Süddeutschen Klassenlotterie (SKL) stammten. Dies löste eine intensive **öffentliche Debatte** aus über

- die Datenverarbeitung bei Callcentern,
- deren Kaltakquise am Telefon (sog. Cold Calls),
- das Fingieren von Verträgen und das unberechtigte Abbuchen von Girokonten,
- den Verkauf von Kontodaten bzw. den legalen und den illegalen Adressenhandel sowie
- die Sicherheit von Kundendaten auch in seriös erscheinenden Unternehmen.

Im Rahmen dieser Diskussion kamen weitere **illegale Datenbestände** ans Licht, die in vergleichbaren Zusammenhängen entstanden und genutzt wurden. Der bisher insofern markanteste Fall war der Aufkauf von 6 Millionen Datensätzen im Auftrag der Verbraucherzentrale Bundesverband (vzbv) auf dem Schwarzmarkt für einen Preis von 850 Euro, wobei 4 Millionen der Datensätze Kontodaten enthielten.

Die Daten wurden von den **Verbraucherschutzverbänden** dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) und dem Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) weitergegeben, die die Daten analysierten und an die zuständigen **Staatsanwaltschaften** verbunden mit einem Strafantrag nach § 44 Bundesdatenschutzgesetz (BDSG) weitergaben. Eingeschaltet wurde weiterhin die in einigen Fällen örtlich zuständige Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW).

II. Die Vorgehensweise beim illegalen Datenhandel

Der bei den vorhandenen Datensätzen regelmäßig erfolgte Ablauf stellt sich nach den bisherigen Erkenntnissen wie folgt dar: Die Kundendaten einschließlich der Kontoverbindung wurden auf unterschiedliche Weise erlangt. Die größten Bestände stammen offensichtlich aus Glücksspielunternehmen. Da diese Unternehmen angeben, die Daten nicht verkauft zu haben, wird derzeit davon ausgegangen, dass entweder unzuverlässige Mitarbeiter Firmendatenbestände kopiert und an Adresshändler weiterverkauft haben oder im Rahmen von Callcenteraufträgen nach Abschluss der Aufträge die Daten nicht gelöscht, sondern angesammelt wurden. Als weitere **Datenquellen** kommen in Frage: Eigenangaben von Verbrauchern im Rahmen von telefonischen Kaltakquisen durch Callcenter, Daten aus der Inanspruchnahme von Internetdiensten, Angaben aus dem Zeitschriftenvertrieb, aus Spendensammlungen, aus Preisausschreiben u.Ä., Auszüge aus Kundendatenbeständen sonstiger Unternehmen.

Die erhobenen Daten werden offensichtlich in vielen Fällen an **Adresshändler** weitergegeben, die diese auf dem Schwarzmarkt – wiederum v.a. an **Callcenter** – weiterverkaufen. Die Callcenter nutzten diese einschließlich der Kontodaten für die weitere Telefonakquise oder für

das **Fingieren von Verträgen** (in den unterschiedlichsten Branchen: z.B. Lotterie, Telekommunikation, Zeitschriftenvertrieb, Online-Angebote, Spenden). Die Daten werden daraufhin von den Callcentern an die Unternehmen weitergegeben, für die tatsächlich oder vermeintlich Verträge abgeschlossen werden, die hierfür Provisionen bezahlen und von den Konten der (vermeintlich) gewonnenen Kunden abbuchen. Soweit bisher bekannt, werden die **Kontoabbuchungen** von den Banken regelmäßig ungeprüft akzeptiert, selbst dann, wenn es sich um Massenabbuchungen handelt und auf Grund von Widersprüchen von Kunden und dadurch notwendigen Rückbuchungen Hinweise darauf bestehen, dass tatsächlich keine Abbuchungsermächtigungen der Kunden vorliegen. Rückbuchungen werden innerhalb einer Frist von 6 Wochen ohne weitere Hinterfragung von den Banken durchgeführt. Erfolgen Widersprüche später, so ist es den Betroffenen zumeist nicht mehr möglich, das überwiesene Geld zurückzuerhalten.

III. Datenschutzrechtliche Bewertung

Datenschutzrechtlich ist die Nutzung von Kontodaten für Werbezwecke unzulässig, wenn die Betroffenen hierzu nicht ausdrücklich ihre **Einwilligung** (§ 4a BDSG) erteilt haben. Es ist bisher noch kein einziger Fall bekannt geworden, dass ein Betroffener der Nutzung der Kontodaten für Werbezwecke zugestimmt hätte.

Die Nutzung von personenbezogenen Daten für **Werbezwecke** ist derzeit bei Vorliegen eines gesetzlich definierten Datensatzes (Name, Adresse, Geburtsjahr, Branche, Gruppenzugehörigkeit) besonders rechtlich privilegiert (§ 28 Abs. 3 Nr. 3 BDSG). Darüber hinausgehend wird in der Praxis die Nutzung von Daten für zulässig angesehen, wenn keine „schutzwürdigen Interessen“ der Betroffenen überwiegen (§ 28 Abs. 1 Nr. 2 BDSG). Dies ist bei der Nutzung von Kontodaten unzweifelhaft der Fall. Überwiegende schutzwürdige Interessen bestehen auch z.B. bei Daten über die politische Überzeugung, Gesundheit oder sexuelle Orientierung (vgl. § 3 Abs. 9 BDSG). Abgesehen von diesen klaren Fällen gibt es eine große Grauzone und viel rechtliche Unsicherheit. Da die Abwägung von Unternehmensinteressen an Werbung und Schutzinteressen der Betroffenen von den Unternehmen selbst vorgenommen wird, fällt diese regelmäßig zugunsten der Werbenutzung aus. Dadurch werden Verbraucherinteressen de facto massiv beeinträchtigt.

Die Bereitstellung von Daten an Callcenter erfolgt in vielen Fällen als **Datenverarbeitung im Auftrag** (§ 11 BDSG). Auftraggeber sind zumeist große Unternehmen, die die Callcenter mit der Akquise, der Kundenrückgewinnung oder der Kundenbetreuung beauftragten. Hierfür werden oft Kundendaten des Auftrag gebenden Unternehmens dem Callcenter bereitgestellt, u.a. auch Kontodaten. Diese Daten müssten nach Beendigung des Auftrags vollständig wieder gelöscht oder zurückgegeben werden. Eine Nutzung dieser Daten für **andere Zwecke** (z.B. eigene Zwecke des Callcenters) ist unzulässig. Es bestehen Hinweise darauf, dass dies von vielen Callcentern nicht beachtet wird und dass ein Zusammenführen der Datenbestände erfolgt.

Im Fall einer Datenverarbeitung im Auftrag durch ein Callcenter müsste ein schriftlicher Vertrag präzise die in Auftrag gegebene Datenverarbeitung und die zu treffenden technisch-organisatorischen Maßnahmen festlegen. Die **Einhaltung dieser vertraglichen Vorgaben** ist vom Auftrag gebenden Unternehmen präzise zu überwachen. Der Auftragnehmer ist sorgfältig auszuwählen (§ 11 Abs. 2 BDSG). Diese Pflichten wurden bei der Einschaltung von Callcentern offensichtlich sehr oft missachtet: Werden z.B. dem Auftraggeber Missstände (Stornos wegen fingierter Verträge, Mängel bei der Datensicherheit, Datenlecks) bekannt, so müsste der Auftraggeber umgehend entweder den Vertrag kündigen oder auf die Behebung der Mängel drängen und dies überprüfen. Dies scheint oft nicht zu geschehen.

Es gehört zu den **Pflichten der Auftragnehmer**, also der Callcenter, die Daten nur im Rahmen der Weisungen des Auftraggebers und nur für die festgelegten Zwecke zu verarbeiten. Sie

müssen die technisch-organisatorischen Anforderungen (§ 9 BDSG mit Anlage) beachten. Ist ein Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen das Gesetz verstößt, hat er den Auftraggeber darauf unverzüglich hinzuweisen (§ 11 Abs. 3 BDSG). Diese Pflichten werden anscheinend von Callcentern oft nicht beachtet: Die Speicherung der zur Verfügung gestellten Daten und Nutzung für andere Zwecke ist unzulässig. Callcenter-Agenten berichteten immer wieder, dass es ihnen möglich ist, sich die bearbeiteten Daten über offene Schnittstellen (CD-Brenner, USB-Anschluss, Versendung durch Mail) zu verschaffen und weiterzugeben. Immer wieder gilt dies nicht nur für die bearbeiteten Einzeldatensätze, sondern für gesamte Kundendatenbestände. Es ist bisher noch kein Fall bekannt geworden, dass ein Callcenter einen Auftrag zurückgewiesen hätte, weil dieser gegen Datenschutzrecht verstößt.

Die materiell unzulässige Datenverarbeitung stellt eine **Ordnungswidrigkeit** dar, die nach § 43 Abs. 2, 3 BDSG mit einem Bußgeld bis zu 250.000 Euro geahndet werden kann. Die Ahndung erfolgt regelmäßig durch die Datenschutzaufsichtbehörden (z.B. in Schleswig-Holstein durch das ULD).

Erfolgt eine solche Handlung vorsätzlich und gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder zu schädigen, so liegt eine **Straftat** vor, die mit Freiheitsstrafe bis zu zwei Jahren bestraft werden kann (§ 44 Abs. 1 BDSG). Diese Voraussetzungen sind in den bekannt gewordenen Fällen regelmäßig erfüllt. Die Taten werden nur auf Antrag verfolgt. Antragsberechtigt sind die Betroffenen, die verantwortlichen Stellen, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) und die Aufsichtsbehörden (§ 44 Abs. 2 BDSG), also z.B. das ULD, der BlnBDI oder die LDI NRW. Sowohl verarbeitende Stellen (z.B. Telekom, SKL) wie auch Aufsichtsbehörden haben entsprechende Strafanträge gestellt.

IV. Änderungsbedarf im Datenschutzrecht

Derzeit finden **zwei Gesetzgebungsverfahren** statt, die einen direkten Bezug zu den konkreten Sachverhalten haben. Beide Gesetzentwürfe wurden von der Bundesregierung auf ihrer 114. Kabinettssitzung am 30.07.2008 beschlossen. Ein „Gesetzentwurf zur Bekämpfung unerlaubter Telefonwerbung und zur Verbesserung des Verbraucherschutzes bei besonderen Vertriebsformen“, der von der allgemeinen Zielsetzung zwar begrüßt, aber in der Reichweite von Bundesländern und Verbraucherschützern kritisiert wurde, enthält bisher keine datenschutzrechtlichen Regelungen. Der „Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes“ erfasst lediglich die Bereiche Auskunfteien und Scoring.

Die Forderung zur Aufnahme eines Grundrechts auf Datenschutz in das Grundgesetz (so z.B. Bundestagsfraktion Bündnis 90/Die Grünen) hat mit dem konkreten Sachverhalt direkt nichts zu tun. Verfassungsrechtlich geregelt werden könnte und sollte – was indirekt eine Auswirkung auf entsprechende Fälle hätte – eine **Grundgesetzregelung**, die die Unabhängigkeit und eine ausreichende Ausstattung (institutionelle Absicherung) der Datenschutzkontrolle gewährleistet. Bisher sind viele Aufsichtsbehörden in die Innenverwaltung (Hamburg: Justizverwaltung) integriert, was die Unabhängigkeit der Datenschutzkontrolle in Frage stellt.

Es wurde von vielen Seiten der Vorschlag gemacht, die Weitergabe von personenbezogenen Daten für Werbezwecke generell unter Einwilligungsvorbehalt zu stellen, also von der **informierten Einwilligung der Betroffenen** (§ 4a BDSG) abhängig zu machen (u.a. Bundesverbraucherminister – BMELV – Horst Seehofer; Bundesjustizministerin – BMJ – Brigitte Zypries). Dies wird von Datenschutzbeauftragten seit Jahren immer wieder gefordert. Die bisherige Privilegierung der Werbenutzung ist verfassungsrechtlich fragwürdig (vgl. Weichert in Taeger/Wiebe, Informatik-Wirtschaft-Recht, Festschrift für Kilian, 2004, S. 295) und rechtspolitisch anachronistisch. Die Erfahrungen mit den bisherigen Regelungen ist, dass sie zu weit sind und in der Praxis nicht beachtet werden (dies gilt für die Abwägungsklausel in § 28 Abs. 1 Nr. 2 BDSG – s.o. – und in großem Umfang für die Hinweispflichten und

Widerspruchsrechte in § 28 Abs. 4 BDSG).

Die Informationspflicht von Betroffenen bei Datenpannen wird in jüngerer Zeit intensiv diskutiert, nachdem dieses aus den USA kommende Datenschutzinstrument (**breach notification**) von der EU-Kommission in den Vorschlag einer Telekommunikations-Datenschutzrichtlinie (ePrivacy-Directive) Eingang fand. Der Vorschlag wird u.a unterstützt von BMELV Seehofer und BMJ Zypries. Die Voraussetzungen einer Informationspflicht müssen noch geklärt werden um zu verhindern, dass Menschen unnötig beunruhigt werden und ein unverhältnismäßiger Aufwand bei den Unternehmen entsteht.

Vorgeschlagen wird weiter zu verbieten, dass Firmen die Zustimmung zur übermäßigen Datennutzung zur Bedingung für den Vertragsabschluss machen. BMELV Seehofer hat ein solches **Koppelungsverbot** zumindest für marktbeherrschende Unternehmen gefordert. Ein derartiges Verbot gibt es bisher nur im Telemedienrecht (§ 12 Abs. 3 TMG). Da aber das Abfordern von Daten, die für die Vertragsabwicklung nicht benötigt werden, sich nicht auf diese Branche beschränkt, ist ein solcher Vorschlag sehr zu begrüßen.

Von Vielen wird vorgeschlagen, die **Strafen** für unzulässige Datenverarbeitung stark heraufzusetzen. Tatsächlich wurde der bisherige Sanktionsrahmen weder im Bereich des Ordnungswidrigkeitenrechts noch im Strafrecht vollständig ausgeschöpft. Dies lag vor allem daran, dass die Sanktionswürdigkeit bisher von Seiten der zuständigen Staatsanwaltschaften nicht hinreichend anerkannt wurde. Dies hat sich offenbar auf Grund der jüngsten Ereignisse und der öffentlichen Resonanz hierauf geändert. Es ist absehbar, dass der Sanktionsrahmen mittelfristig nicht mehr ausreichen wird. Zudem wird mit einer Erhöhung des Sanktionsrahmens die Bedeutung der Delikte politisch zum Ausdruck gebracht. Während bisher Datenschutzdelikte eher als individuelle Verstöße betrachtet wurden, handelt es sich bei den in jüngster Zeit bekannt gewordenen Delikten zweifellos um eine besondere Form der Wirtschaftskriminalität, die in einer Gesellschaft, in der wirtschaftlich relevante informationstechnische Kommunikation eine zunehmende Rolle spielt, immer gefährlicher zu werden droht. Die von BMJ Zypries erwogene Abschaffung des Antragserfordernisses und die Bewertung von Datenschutzverstößen als Offizialdelikte ist zu begrüßen.

Vorgeschlagen wird weiterhin, den durch Datenmissbrauch entstandenen Gewinn wieder einzuziehen (BMJ Zypries; Bündnis 90/Die Grünen im Bundestag). Diese **Gewinnabschöpfung** setzt die weitgehende Ausermittlung der Sachverhalte voraus. Angesichts des Dunkelfelds beim Datenmissbrauch und der bisherigen Vollzugs- und Ermittlungsdefizite kann diese Maßnahme erst am Ende der Verfahren relevant und auch wirksam werden. Es kann daher noch nicht abgeschätzt werden, welche praktische Bedeutung ihr zukommen kann.

Zu Recht werden Defizite im Bereich der **Datensicherheit** moniert. So wird vorgeschlagen, im Fall des Datenhandels deren Nutzung zu dokumentieren (so BMELV Seehofer). Tatsächlich ist es derzeit ein Problem der Datenschutzkontrolle, dass verantwortliche Stellen oft weder die Herkunft von Daten noch die Empfänger im Fall von Übermittlungen dokumentieren, so dass Datenflüsse nicht nachvollzogen werden können und das Auskunftsrecht der Betroffenen leerläuft. Derartige Dokumentationspflichten bestehen schon heute, auch wenn sie nicht gesetzlich ausdrücklich geregelt sind (abgeleitet z.B. aus § 9 BDSG). Fraglich ist, ob eine singuläre Regelung sinnvoll ist, da die Vollzugsdefizite nicht nur im Bereich des Datenhandels für Werbezwecke bestehen. Eine massive rechtliche Verbesserung würde dadurch erreicht, dass die Ziele der technisch-organisatorischen Maßnahmen – wie in vielen Landedatenschutzgesetzen (LDSG) – auch ausdrücklich in das BDSG aufgenommen würden: Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit, Transparenz. Damit würde zugleich eine Konkretisierung des jüngst vom Bundesverfassungsgericht (BVerfG) geschaffenen Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erfolgen (U.v. 27.02.2008, Az. 1 BvR 370/07 u.a.).

Bisher wird von den Gerichten in Frage gestellt, dass es sich beim Datenschutzrecht um **verbraucherschützende Normen** handelt, die auch von den Verbraucherzentralen gerichtlich durchgesetzt werden könnten (dazu Weichert VuR 2006, 377, siehe auch 452). Obwohl diese Rechtsprechung schon nach derzeitiger Gesetzeslage kaum haltbar ist, wäre es im Interesse einer klaren Aufgabenzuordnung und der Rechtssicherheit geboten, gesetzlich klarzustellen, dass den Verbänden auch eine Verbraucherdaten schützende Funktion zukommt.

Im Datenschutzrecht besteht darüber hinausgehender **weiterer Novellierungsbedarf**, der mit dem aktuellen Missbrauch von Kontodaten nicht in direktem Zusammenhang steht. Das BDSG ist in seiner aktuellen Fassung nicht mehr an die technischen Gegebenheiten des Internet angepasst. Seit mehreren Jahren ist unbestritten, dass es einer umfassenden Modernisierung des allgemeinen Datenschutzrechtes bedarf. Dies führt insbesondere auch im Bereich des Datenschutzes für Verbraucherinnen und Verbraucher zu rechtlichen Verunsicherungen. Dieses Thema ist Gegenstand der Diskussion der am 01.09.2008 in Kiel stattfindenden Sommerakademie „Internet 2008 – alles möglich, nichts privat?“.

V. Sonstige datenschutzpolitische Forderungen

Der Vorschlag, die Datenschutzkontrolle zu verbessern, kann nur nachhaltig unterstützt werden. Derzeit sind die **Aufsichtsbehörden** nach § 38 BDSG personell und sachlich so ausgestattet, dass diese ihre Aufgaben nicht ansatzweise befriedigend erfüllen können. Es gibt – soweit bekannt – derzeit kein Bundesland, in dem eine zweistellige Zahl von Personen für die Datenschutzaufsicht im Privatbereich eingesetzt wird. Der Umstand, dass diese öffentlich Bediensteten zumeist mehrere 100.000 Betriebe überprüfen sollen, erklärt u.a. die bestehenden Vollzugsdefizite.

Der Vorschlag des Bundes Deutscher Kriminalbeamten (BDK), bei den Datenschutzaufsichtsbehörden **besondere Ermittlungsgruppen** einzurichten, die technische und rechtliche Kompetenz sowie Ermittlungserfahrungen miteinander kombinieren und für die Strafverfolgungsbehörden die notwendigen Grundlagen für weitere strafrechtliche Ermittlungen liefern können, ist ein richtiger Ansatz. Es kann festgestellt werden, dass die Sachverhalte regelmäßig länderübergreifend und von hoher technischer Komplexität sind. Über die organisatorische Einbindung, die genauen Aufgaben und Befugnisse muss aber eine weitere Diskussion erfolgen. Es muss verhindert werden, dass derartige Ermittlungstrupps im Vorfeld von Gefahren und Straftaten tätig werden, so wie dies in anderen Bereichen durch die Polizei der Fall ist.

VI. Verbraucherpolitische Forderungen

U.a. die Verbraucherschutzministerkonferenz hat vorgeschlagen, die Wirksamkeit von telefonisch geschlossenen Verträgen von einer **schriftlichen Bestätigung** abhängig zu machen. Dies ist aus Datenschutzsicht zu begrüßen, da diese Bestätigung die Transparenz für die Betroffenen dadurch erhöht, dass diese Kenntnis erlangen, welches Unternehmen welche (Vertrags-) Daten über sie verarbeitet.

Sobald erste Beschwerden oder mehrfache Stornos von Abbuchungen in einer Bank über eine abbuchende Firma vorliegen, sollten alle weiteren Transaktionen gestoppt, als Grundlage die schriftliche Ermächtigung der Betroffenen eingefordert und die Betroffenen informiert werden. Diese Pflichten dürften derzeit schon den Banken zukommen (vgl. Urteil des Bundesgerichtshofes – BGH – v. 06.05.2008, Az. XI ZR 56/07). Die Banken sind sich aber offensichtlich dieser Pflichten bei entsprechendem **Verdacht** bisher nicht hinreichend bewusst. Eine Konkretisierung dieser Pflichten ist auch im Sinne des Datenschutzes, da mit ihnen nicht nur unzulässige Geld-, sondern auch Datentransaktionen vermieden werden können.

Die Erstellung von **Warndateien über Unternehmen**, bei denen der begründete Verdacht von

Verbraucherschutzverstößen besteht, ist aus Datenschutzsicht möglich. Derartige Dateien über Verbraucher zum Schutz von Unternehmen bestehen schon heute und finden grds. in § 29 BDSG ihre rechtliche Grundlage. Es ist erstaunlich, dass bzgl. der erheblich größeren Gefährdung durch Unternehmen ein solches Angebot zum Schutz der Verbraucher bisher nicht besteht. Selbstverständlich müssen die strengen rechtlichen Anforderungen des § 29 BDSG, die heute oft nicht beachtet werden, erfüllt sein.

Dr. Thilo Weichert
Leiter des ULD

Kontakt & Impressum Datenschutzerklärung