

# Illegaler Datenhandel

*Das Geschäft mit Ihren Bankdaten*



## Inhaltsverzeichnis

|                                                                                                             |    |
|-------------------------------------------------------------------------------------------------------------|----|
| A. Der Handel mit den Kontodaten .....                                                                      | 2  |
| 1. Die „Masche“: Fingierte Verträge, Abonnements und Gewinnversprechen.                                     |    |
| 2. Wie kommen die an meine Daten?                                                                           |    |
| 3. Wieso sind Kontodaten ohne Einzugsermächtigung nutzbar?                                                  |    |
| B. Von meinem Konto wurde unberechtigt Geld abgebucht – Was kann ich tun?.....                              | 9  |
| 1. Erste Priorität: Geld zurück!                                                                            |    |
| 2. Kann ich meine Daten löschen lassen?                                                                     |    |
| 3. Kann ich Strafanzeige stellen?                                                                           |    |
| C. Angeblich soll ich einen Vertrag/ein Abonnement abgeschlossen haben – Wie soll ich mich verhalten? ..... | 12 |
| 1. Soll ich auf die angebliche Forderung reagieren?                                                         |    |
| 2. Ist ein Widerruf erforderlich – Wie gehe ich am besten vor?                                              |    |
| D. Wie kann ich mich präventiv schützen? .....                                                              | 13 |
| 1. Worauf muss ich bei der Preisgabe meiner persönlichen Daten achten?                                      |    |
| 2. An wen kann ich mich wenden, wenn ich Fragen zum Thema habe?                                             |    |
| Kontakt.....                                                                                                | 16 |
| Weitere Broschüren.....                                                                                     | 16 |

Impressum:

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)  
Holstenstraße 98, 24103 Kiel, [www.datenschutzzentrum.de](http://www.datenschutzzentrum.de)

Stand: August 2009

## **A. Der Handel mit den Kontodaten**

### **1. Die „Masche“: Fingierte Verträge, Abonnements und Gewinnversprechen**

Verbraucherschützer und Datenschutzbehörden erhalten eine Vielzahl von Beschwerden von Verbraucherinnen und Verbrauchern über unerwünschte Telefonanrufe. In letzter Zeit verschärft sich die Problematik: Besorgte Verbraucher beklagen nicht nur, dass sie von dubiosen Firmen per Telefon kontaktiert wurden. Während der Telefonate stellt sich teilweise heraus, dass die Kontodaten des Verbrauchers beim Anrufer bereits bekannt sind.

#### ***Was wollen die Anrufer erreichen?***

Die Anrufer verfolgen insbesondere zwei Zwecke:

Den Verbrauchern sollen am Telefon persönliche Daten entlockt werden.

und / oder

Den Verbrauchern sollen Gewinnspielabonnements, die Teilnahme an Lotterien oder sonstige Dienstleistungsverträge aufgeschwatzt oder untergeschoben werden.

Selbst wenn die Verbraucher einem Vertragsabschluss **nicht** zustimmen, werden die Verträge zum Teil fingiert.

#### ***Welche „Geschäftsmodelle“ gibt es?***

Die erste Kontaktaufnahme erfolgt zumeist per Telefon. Die Betroffenen sollen Gewinnspielverträge, -abonnements oder Lotterieteilnahmen erwerben. Zum Teil werden auch Warenproben bzw. angebliche Gratisdienstleistungen angeboten oder Gewinnzusagen gemacht, um auf diesem Wege in den Besitz persönlicher Daten und insbesondere der Kontodaten der Angerufenen zu ge-

langen. Die Anrufer versuchen, die Betroffenen in Gespräche zu verwickeln und Ihnen so viele Informationen wie möglich zu entlocken. So wird z.B. häufig eine falsche Kontoverbindung genannt, so dass der überrumpelte Verbraucher ohne nachzudenken die falschen Daten berichtet. Auf diesem Wege gelangt der Anrufer an den korrekten Datensatz.

„Sie sind doch bei der Sparkasse X“ „Nein, ich bin bei der Volksbank Y!“

➔ Das **Ablenkungsmanöver**: Der Betroffene fragt gar nicht mehr nach, woher die Informationen stammen, sondern sieht sich vorrangig in der Pflicht, die Daten zu korrigieren.

Häufig liegen den Anrufern die Kontodaten bereits vor. Diese stammen aus illegalen Quellen und werden dazu verwendet, den Verbrauchern Verträge unterzuschieben. In diesen Fällen haben die Anrufer nicht selten die Vorgabe, sich die Kontodaten noch einmal vom Betroffenen mitteilen zu lassen. Damit können sie die vorhandenen Daten auf Aktualität überprüfen. Wahlweise wird vom anderen Ende der Leitung her so getan, als existiere bereits ein Lotterieabonnementvertrag.

„Wir haben doch im letzten Monat mit Ihrem Mann ein Abonnement abgeschlossen.“

Wenn die Angerufenen daraufhin erklären, dass sie das Abonnement nicht abgeschlossen haben bzw. dieses nicht haben wollen, bieten die Anrufer an, das Abonnement zu kündigen. Allerdings – so häufig die Aussage – ginge dies erst zum nächsten Monatsersten bzw. mit einer dreimonatigen Kündigungsfrist.

„Wir buchen dann aber noch dreimal ab.“

➔ Das **Ablenkungsmanöver**: Die eigentliche Streitfrage, ob ein Abonnement überhaupt abgeschlossen wurde, hat der Anrufer damit geschickt umschifft. Er weist den Betroffenen auf die Kündigungsmöglichkeit hin und nutzt die Erleichterung und Unsicherheit der Angerufenen aus: Angesichts der in Aussicht gestellten Möglichkeit, aus dem vermeintlichen Abonnement schneller wieder herauszukommen als im ersten Schrecken gedacht, akzeptieren die Betroffenen zumeist, dass zukünftig „nur“ noch ein, zwei oder drei Abbuchungen stattfinden.

Aktuell gibt es auch Firmen, die mit der Angst der Verbraucher spielen: Ausgerechnet das Bedürfnis der Betroffenen, ihre Daten zu schützen, nutzen solche Anrufer aus. Sie geben sich als Mitarbeiter von nicht existierenden Datenschutz-Clubs, Verbraucher-Vereinen oder „Datensperrzentralen“ aus und konfrontieren die Betroffenen am Telefon mit der Behauptung, sie hätten deren Kontodaten im Internet entdeckt. Die Anrufer bieten sodann an, sich gegen einen monatlichen Beitrag von knapp 50 € um den Schutz der Daten zu „kümmern“. Das Problem ist, dass die Daten gar nicht aus dem Internet stammen. Vielmehr arbeiten auch solche Firmen mit illegal angekauften Kontodaten. Sie nutzen die Bestürzung der Angerufenen aus, um eine Dienstleistung zum Schutze der Daten im Abonnement anzubieten.

➔ Der **Überrumpelungseffekt**: Im Regelfall handelt es sich bei solchen Angeboten um unseriöse Offerten. Erkennbar ist dies bereits daran, dass diese Firmen die Verbraucher ungebeten per Telefon kontaktieren, ohne mitzuteilen, woher sie die Telefonnummern haben, um dann gegen Geld eine Dienstleistung zum angeblichen Schutz der Betroffenen anzubieten. Die Anrufer nutzen dabei das Gefühl der Vertrauenswürdigkeit aus, das Verbraucher grundsätzlich mit den Begriffen „Verbraucherschutz“ und „Datenschutz“ verbinden. Sie überrumpeln die Betroffenen mit der Dar-

stellung eines Szenarios, das die Angerufenen am Telefon gar nicht so schnell überprüfen können.

Zum Teil werden Verbraucher auch auf schriftlichem Wege angesprochen. Dabei werden dann Sätze verwendet wie:

„Wir bestätigen Ihre kostenpflichtige Teilnahme am Gewinnspiel X.“ Und gleich darunter sind die Kontodaten der Angeschriebenen notiert.

Manchmal werden auch die angeblichen Vertragsschlüsse am Telefon auf schriftlichem Wege bestätigt. Dabei tauchen auch die Kontodaten in den Anschreiben auf. Häufig als Beweis dafür, dass der Vertragsschluss am Telefon tatsächlich stattgefunden hat. Die Argumentation ist perfide:

„Wir hätten die Kontodaten ja nicht, wenn Sie uns diese nicht selbst am Telefon genannt hätten.“

Selbst für den Fall, dass der Verbraucher weder auf das Vertrags- oder Dienstleistungsangebot noch auf ein angeblich bereits bestehendes Abonnement eingeht, wird zum Teil trotzdem abgebucht. Der Anrufer ist im Besitz der Kontodaten. Durch Vortäuschung einer bestehenden Einzugsermächtigung wird Geld vom Konto eingezogen (näheres dazu siehe unter Punkt A. 3. „Wieso sind Kontodaten ohne Einzugsermächtigung nutzbar?“).

### ***Warum funktioniert das?***

Die Masse macht's! Wenn nur ein Bruchteil der Angerufenen sich zu einem Vertragsschluss überreden lässt, das vermeintliche Abonnement erst mit dreimonatiger Frist kündigt oder einer unberechtigten Abbuchung von seinem Konto nicht widerspricht, lohnt sich das „Geschäft“ angesichts der Masse der Anrufe.

Warum werden die Verbraucher aber überhaupt angerufen? Wenn die Kontodaten auch ohne Vertragsschluss zur Abbuchung genutzt werden können, hat der Anruf doch eher den kontraproduktiven Effekt, dass die Betroffenen in Alarmbereitschaft versetzt werden?

Bemerken die Betroffenen die Abbuchung von ihren Konten und hätte gar keine vorhergehende Kontaktaufnahme per Telefon stattgefunden, ist wahrscheinlich klar: Hier stimmt etwas nicht!

Erinnert sich der Angerufene hingegen an einen Anruf und ist die Erinnerung an den Inhalt des Telefongesprächs aufgrund des Zeitablaufs gegebenenfalls nur noch vage vorhanden, kommen die Betroffenen eher ins Zweifeln: Haben sie am Telefon möglicherweise doch „Ja“ gesagt, um den Anrufer möglichst schnell abzuwimmeln? Einige Betroffene glauben gehen möglicherweise auch davon aus, dass sie keine Chance haben, das Geld zurückzubekommen. Sie nehmen vielleicht an, dass sie beweisen müssten, einem Vertragsschluss **nicht** zugestimmt zu haben und sehen sich dazu nicht in der Lage. Diese Unsicherheit wird systematisch ausgenutzt. Häufig werden auch gezielt ältere Menschen angerufen.

Zum Teil kommen die Anrufe von Callcentern oder sonstigen Vertriebspartnern, die von anderen Firmen beauftragt wurden. Diese Callcenter erhalten von den Auftraggebern Provisionen für Vertragsabschlüsse am Telefon. Um dem Auftraggeber erfolgreiche Vertragsabschlüsse zu übermitteln und die Provisionen zu kassieren, werden Verträge fingiert. Der Telefonanruf dient gegenüber dem Auftraggeber als Nachweis für die Kontaktaufnahme mit dem Betroffenen.

Auch wer sich wehrt, stößt häufig zunächst auf Widerstand. Der Anruf wird dann im Nachhinein als „Beweismittel“ angeführt. Per Einzelverbindungs nachweis wird die telefonische Kontaktaufnahme

me nachgewiesen. Als weiteres „Argument“ wird behauptet: Der Verbraucher muss die Kontodaten am Telefon selbst preisgegeben haben. Nur so hätte man in den Besitz derselben gelangen können.

Dass die Daten nicht vom Betroffenen selbst angegeben wurden, sondern aus illegalen Quellen vor dem Anruf beschafft wurden, bleibt dabei natürlich unerwähnt.

## **2. Wie kommen die an meine Daten?**

Eine einzige Antwort auf diese Frage gibt es nicht. Die Wege der illegalen Datenbeschaffung sind vielfältig:

Ein großer Teil von illegalen (Konto-)Daten stammt offensichtlich aus den Beständen von Glücksspielunternehmen. Da diese Unternehmen angeben, die Daten nicht verkauft zu haben, gehen wir derzeit davon aus, dass entweder unzuverlässige Mitarbeiter Firmendatenbestände kopiert und an Adresshändler weiterverkauft haben oder Daten an Callcenter weitergegeben wurden, die diese nach Abschluss des Auftrages nicht gelöscht bzw. zurückgegeben haben.

Als weitere **Datenquellen** kommen in Frage: Eigenangaben von Verbrauchern im Rahmen von telefonischen Kaltakquisen, Daten aus der Inanspruchnahme von Internetdiensten und insbesondere auch Internetgewinnspiele, 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 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.

### **3. Wieso sind Kontodaten ohne Einzugsermächtigung nutzbar?**

Ohne eine zuvor erfolgte Einzugsermächtigung des Kontoinhabers dürfen Dritte keine Beträge vom fremden Konto abbuchen.

Dennoch ist es bei diesem sog. Lastschriftverfahren möglich, dass Beträge abgebucht werden, ohne dass eine Einzugsermächtigung vorlag.

Das Verfahren für die Lastschrift ist bundeseinheitlich seit 1963 im sog. Lastschriftabkommen geregelt und funktioniert so:

Der aufgrund der erteilten Einzugsermächtigung Einzugsberechtigte übergibt seinem Geldinstitut ein als Lastschrift ausgewiesenes Formular mit dem Namen und der Bankverbindung des Zahlungspflichtigen, sowie dem abzubuchenden Betrag. Das Geldinstitut wendet sich daraufhin an die Empfängerbank des Zahlungspflichtigen, welche aufgrund der erklärten Einzugsermächtigung eine Belastung des Kontos der Zahlungspflichtigen vornimmt.

Im Massenverfahren der Lastschrifteinlösung können solche Stellen Beträge von fremden Konten per Lastschrifteinzug abbuchen, die durch die Bank im Wege einer sog. Inkassovereinbarung zugelassen wurden. Die Ermächtigung des Kontoinhabers zum Einzug durch Lastschrift wird im Einzelfall regelmäßig nicht überprüft. Der Zahlungsempfänger muss sich nur verpflichten diese auf Verlangen vorzulegen.

Zum Schutz vor unberechtigten Kontobelastungen kann der Kontoinhaber innerhalb einer 6-Wochenfrist bei seinem kontoführenden Institut der Abbuchung widersprechen. Die kontoführende Stelle ist dann verpflichtet, die Rückbuchung zu veranlassen. Eine Einzugsermächtigung fehlt, wenn die Ermächtigung nicht erteilt oder widerrufen wurde oder wenn der abgebuchte Betrag nicht geschuldet wird.

## **B. Von meinem Konto wurde unberechtigt Geld abgebucht – Was kann ich tun?**

### **1. Erste Priorität: Geld zurück!**

Der Geschädigte sollte sofort, nachdem er von der rechtswidrigen Lastschriftabbuchung Kenntnis erlangt hat, diese bei seinem Geldinstitut widerrufen. Dieser Widerruf muss nicht begründet werden.

Der Widerruf ist häufig im Wege des Online-Banking möglich, telefonisch oder mündlich direkt am Schalter.

Die kontoführende Stelle ist dann verpflichtet, die Rückbuchung zu veranlassen. Erfolgt der Widerruf des Kunden innerhalb einer Frist von 6 Wochen, wobei die Frist am Folgetag der Abbuchung beginnt, wird der abgebuchte Betrag problemlos dem Konto wieder gutgeschrieben.

Da die Abbuchung ohne vorher erteilte Einzugsermächtigung erfolgte, werden die Verwaltungskosten der Rückbuchung dem widerrechtlich Abbuchenden berechnet.

Problematisch ist es, wenn der Kontoinhaber erst nach Ablauf von 6 Wochen bemerkt, dass eine unzulässige Abbuchung erfolgt ist. Nach Ablauf dieses Zeitrahmens (beginnend mit der Abbuchung), aber noch innerhalb einer (zweiten) 6-Wochenfrist, gerechnet ab dem (regelmäßigen) Rechnungsabschluss des Kontos, muss der

Kontoinhaber bei einem Widerruf mit Schadensersatzansprüchen des eigenen kontoführenden Instituts rechnen.

Die eigene Bank schreibt ihm das Geld zwar wieder auf seinem Konto gut, doch hat sie in der Regel keine Möglichkeit mehr, die Summe von der Empfängerbank zurück zu erhalten. Dort ist das Geld bereits auf dem Konto des Zahlungsempfängers gutgeschrieben worden. Das eigene Geldinstitut kann deshalb einen Schadensersatzanspruch wegen Verletzung der Pflicht des Kontoinhabers, die Kontoauszüge auf ihre Richtigkeit hin zu überprüfen und Einwendungen sofort zu erheben, geltend machen.

Da die Höhe des Schadensersatzanspruchs dem Rückzahlungsanspruch des Kontoinhabers entspricht, hat der geschädigte Kunde in diesen Fällen praktisch keinen durchsetzbaren Anspruch.

## **2. Kann ich meine Daten löschen lassen?**

Gemäß Art. 17 Abs. 1 der Datenschutz-Grundverordnung hat jede Person das Recht, bei unzulässiger Speicherung die Löschung seiner personenbezogenen Daten zu verlangen.

Um diesen Anspruch durchsetzen zu können, müssen die Betroffenen zunächst feststellen, welche Stellen die Daten gespeichert haben und wie diese kontaktiert werden können. In den Fällen der missbräuchlichen Speicherung und Nutzung von Kontodaten ist es für die Betroffenen häufig schon schwierig, die speichernden Stellen genau zu identifizieren. Am Telefon teilen diese regelmäßig nur unvollständig oder undeutlich mit, von welcher Firma sie anrufen. Zugleich wird regelmäßig die Funktion der Rufnummernunterdrückung genutzt, so dass auch keine Anzeige der (Rückruf-)Rufnummer auf dem Display erfolgt. Letztlich besteht zumeist keine Möglichkeit nachzuprüfen, ob die Anrufer tatsächlich diejenigen sind, für die sie sich ausgeben. Selbst wenn die

Anrufer sich namentlich identifizieren, firmieren sie häufig unter Postfachadressen oder es werden falsche Adressen genannt.

Auch wenn die speichernde Stelle identifiziert und dort eine Löschung erreicht werden kann, ist damit nicht viel erreicht: Die Daten sind höchstwahrscheinlich zuvor durch viele Hände geflossen und wurden in einem weit verzweigten Netz an- und verkauft. Nach derzeitiger Rechtslage sind die speichernden Stellen nicht verpflichtet, ihre Datenquellen zu dokumentieren. Es ist für die Betroffenen daher nahezu aussichtslos, die ursprüngliche Quelle ihrer Daten herauszufinden bzw. die Datenkette zurückzuverfolgen, um an jeder Station einen Löschungsanspruch geltend zu machen.

Es besteht die Möglichkeit, die Kontoverbindung für die Teilnahme am Einzugsermächtigungsverfahren zu sperren. Die meisten Banken bieten allerdings nur an, dass dann die Kontoverbindung insgesamt für das Verfahren gesperrt wird. Dies kann in der Praxis zu Problemen führen, insbesondere dann, wenn bestimmte Diensteanbieter, z. B. Stromanlieferanten oder das Telekommunikationsunternehmen keine Zahlung per Dauerauftrag ermöglichen.

In solchen Fällen, in denen unberechtigerweise vom Konto abgebucht wird, sollten Sie Ihre Kontoverbindung umgehend wechseln. Dies gilt auch schon dann, wenn Anhaltspunkte dafür bestehen, dass Ihre Daten illegal im Umlauf sind.

### **3. Kann ich Strafantrag stellen?**

Unbedingt! Sollte von Ihrem Konto unberechtigerweise Geld abgebucht worden sein, kann dies nicht nur einen Betrug darstellen. Auch die unbefugte Datenverarbeitung, in der Absicht sich oder eine andere Person zu bereichern, ist gem. § 42 Bundesdaten-

schutzgesetz unter Strafe gestellt. Der § 42 Bundesdatenschutzgesetz kann in diesen Fällen also ebenfalls verwirklicht sein.

### **C. Angeblich soll ich einen Vertrag/ein Abonnement abgeschlossen haben – Wie soll ich mich verhalten?**

#### **1. Soll ich auf die angebliche Forderung reagieren?**

Ja, und zwar sofort, damit keine Fristen für rechtliche Einwände verstreichen.

Die Verbraucherzentrale bietet auf der Homepage [www.verbraucherzentrale-sh.de](http://www.verbraucherzentrale-sh.de) und in deren Beratungsstellen Musterschreiben an, die verwendet werden können, um sich gegen unberechtigte Forderungen und Rechnungen zu wehren. Das Schreiben sollte zu Beweis Zwecken per Einschreiben, Einwurf oder per Telefax mit Sendeprotokoll übermittelt werden.

Wer sicher ist, keinen Vertrag und auch kein Abonnement abgeschlossen zu haben, oder wer noch nicht 18 Jahre alt (und damit nur beschränkt geschäftsfähig) ist, braucht sich auch bei Zahlungsaufforderungen von Inkassounternehmen und Rechtsanwälten nicht einschüchtern zu lassen und sollte die Forderungen nicht bezahlen.

Bei Fragen hilft die kostengünstige Rechtsberatung in den Beratungsstellen der Verbraucherzentrale weiter, oder es kann die telefonische Service-Nummer-Recht der Verbraucherzentrale genutzt werden. Mehr Informationen zum Beratungsangebot der Verbraucherzentrale unter [www.verbraucherzentrale-sh.de](http://www.verbraucherzentrale-sh.de).

## **2. Ist ein Widerruf erforderlich – Wie gehe ich am besten vor?**

Wer eine Rechnungsforderung erhält und sicher ist, keinen Vertrag und auch kein Abonnement abgeschlossen zu haben, befindet sich in einer guten Rechtsposition.

Denn die Beweislast für den Abschluss und den Inhalt eines Vertrages oder Abonnements trägt hier der Forderungssteller.

Wer sich also einer, wie hier, unberechtigten Rechnungsforderung gegenüber sieht, sollte den Anspruchssteller zunächst auffordern, einen wirksamen Vertragsabschluss nachzuweisen. Zusätzlich sollte eine Vertragsannahme bestritten werden und vorsorglich deren Anfechtung erklärt werden. Sicherheitshalber sollte auch vorsorglich der Widerruf erklärt werden.

Wer sich gegen eine unberechtigte Rechnungsforderung wehren will, kann die Musterschreiben oder das Rechtsberatungsangebot der [www.verbraucherzentrale-sh.de](http://www.verbraucherzentrale-sh.de) nutzen.

## **D. Wie kann ich mich präventiv schützen?**

### **1. Worauf muss ich bei der Preisgabe meiner persönlichen Daten achten?**

Wir empfehlen in jedem Fall sparsam mit personenbezogenen Daten umzugehen. Sollte es Ihnen nicht plausibel erscheinen, warum bestimmte Angaben von Ihnen verlangt werden, fragen Sie nach, wofür die Daten benötigt werden. Wenn Sie auf Nachfrage keine befriedigende, eine ausweichende oder sogar abweisende Antwort erhalten, besteht ein Grund mehr, misstrauisch zu sein. Unternehmen sind gesetzlich verpflichtet, Sie zu informieren, zu welchem Zweck Ihre Daten verwendet werden.

Zudem sollten Sie bei der Weitergabe von Daten am Telefon und im Internet besonders zurückhaltend zu sein. Insbesondere bei Konto- und Telefonverbindungsdaten, empfehlen wir, diese nur dann weiterzugeben, wenn es zwingend notwendig ist und der Vertragspartner zuverlässig erscheint. Bei ungebetenen Telefonanrufen durch Firmen, mit denen Sie zuvor nie zu tun hatten, raten wir, auf eine Preisgabe von persönlichen Daten möglichst ganz zu verzichten.

Die vielen Fälle von unberechtigten Abbuchungen haben gezeigt, wie wichtig es ist, die Kontoauszüge regelmäßig zu kontrollieren. Angesichts der Masse an Kontodaten, die sich illegal im Umlauf befinden, ist niemand hundertprozentig davor geschützt, dass auch seine Daten missbraucht werden. Wir empfehlen daher dringend, die Kontoauszüge stets zu überprüfen und die Bank sofort zu unterrichten, sollten dabei Unregelmäßigkeiten auffallen. Im Fall einer unberechtigten Abbuchung sollten Sie diese umgehend widerrufen und sich zusätzlich auch an die Strafverfolgungsbehörden wenden.

Bei Dienstleistungen im Internet sollten Sie in jedem Fall darauf achten, dass die Firmen sich ihren Webseiten eindeutig identifizieren. Das bedeutet, dass diese die gesetzliche Impressumspflicht erfüllen und (unter anderem) einen vollständigen Firmennamen sowie eine Firmenanschrift angeben.

Für die Teilnahme an Gewinnspielen, Lotterien oder bei anderen Vertragsabschlüssen empfehlen wir dringend, das „Kleingedruckte“ mitzulesen. Seien Sie besonders kritisch, bevor Sie in die Weitergabe Ihrer Daten an Dritte einwilligen. Vorsicht ist geboten, wenn weder die Dritten noch die Zwecke für die Weitergabe konkret benannt werden oder nur ein pauschaler Hinweis erfolgt.

## **2. An wen kann ich mich wenden, wenn ich Fragen zum Thema habe?**

Wenn es um Verbraucherschutzfragen geht, können Sie sich an die örtlichen Verbraucherzentralen wenden.

Für Fragen im Zusammenhang mit der Verarbeitung Ihrer personenbezogenen Daten sind die Datenschutzaufsichtsbehörden die richtigen Ansprechpartner. In jedem Bundesland existiert eine Aufsichtsbehörde für den Datenschutz, die diejenigen nichtöffentlichen Stellen kontrolliert, die ihren Sitz im jeweiligen Bundesland haben. Eine Besonderheit gilt für die Datenverarbeitung bei Unternehmen aus dem Bereich Telekommunikation: Für die Datenschutzkontrolle ist der Bundesbeauftragte für den Datenschutz zuständig, unabhängig davon, wo das Unternehmen seinen Sitz hat.



## **Kontakt**

Verbraucherzentrale Schleswig-Holstein

Beratungsstelle Kiel

Andreas-Gayk-Straße 15, 24103 Kiel

Tel.: +49 (0) 431 590 99- 40

E-Mail: [kiel@verbraucherzentrale-sh.de](mailto:kiel@verbraucherzentrale-sh.de)

[www.verbraucherzentrale-](http://www.verbraucherzentrale-sh.de)

[sh.de](http://www.verbraucherzentrale-sh.de)\\FILE1\\Referatsübergreifendes\\Sonstige-

Themen\\Druckdateien\\BlaueReihe\\6-

Illega-

ler\_Kontodatenhandel\\Druck\\2015\\[www.verbraucherzentrale-sh.de](http://www.verbraucherzentrale-sh.de)

Unabhängiges Landeszentrum für

Datenschutz Schleswig-Holstein (ULD)

Holstenstraße 98, 24103 Kiel

Telefon: +49 (0) 431 988-1200

Telefax: +49 (0) 431 988-1223

E-Mail: [mail@datenschutzzentrum.de](mailto:mail@datenschutzzentrum.de)

[www.datenschutzzentrum.de](http://www.datenschutzzentrum.de)

## **Broschüren zu den Themen**

- Sozialhilfe, Grundsicherung und Arbeitslosengeld II
- Verbraucher-Scoring
- Videoüberwachung und Webkameras
- Internet: Alltag online
- Illegaler Datenhandel
- Soziale Netzwerke

können Sie unentgeltlich bei uns bestellen oder von unserer Homepage unter [www.datenschutzzentrum.de/blauereihe](http://www.datenschutzzentrum.de/blauereihe) herunterladen.