Für Verbraucher und Anbieter

SICHER SURFEN

Die kleine Surf-Fibel der eCommerce Verbindungsstelle Deutschland

Sicher Surfen

Die eCommerce-Verbindungsstelle Deutschland

Nationale Anlaufstelle für Anbieter und Nutzer

Die eCommerce-Verbindungsstelle Deutschland wurde zum 01.01.2003 vom Bundesministerium der Justiz bei Euro-Info-Verbraucher e.V. eingerichtet, um Verbraucher und Anbieter über die rechtlichen Aspekte des elektronischen Geschäftsverkehrs zu informieren. Auf unserer Homepage **www.ecommerce-verbindungsstelle.de** finden Sie umfangreiche Informationen zum Recht im Internet und Hinweise auf weitere Organisationen und Ansprechpartner für speziellere Themen des eCommerce.

Bei konkreten Fragen können Sie sich auch persönlich an uns wenden:

eCommerce-Verbindungsstelle Deutschland
bei Euro-Info-Verbraucher e.V.
Rehfusplatz 11
D - 77694 Kehl
Tel.: 0049 (0)7851 991 48 0
Fax.: 0049 (0)7851 991 48 11
Sprechzeiten: Di-Do 9-12 und 13-17 Uhr

Kontakt: Frau Susanna Münstermann
eMail: info@ecommerce-verbindungsstelle.de

eCommerce

Unter diesen Begriff „electronic commerce“ oder übersetzt „elektronischer Geschäftsverkehr“ fallen **alle Arten von Geschäften**, die auf **elektronischem Weg** abgeschlossen werden können. Dies umfasst unternehmerische Tätigkeiten, wie die Anwerbung von Kunden, die Verarbeitung von persönlichen Daten oder Online-Dienstleistungen.

Sicher Surfen

Inhalt

Einleitung

Einleitung

Sie können sich ein Leben ohne Internetzugang nicht mehr vorstellen? Sie nutzen das Netz zum Einkaufen und für die Urlaubsplanung? Sie lesen Ihre eMails sowie aktuelle Nachrichten und tätigen Überweisungen online? Sie bestellen Ihr neues Sofa oder ersteigern das neue Küchenregal vom PC aus? Dann sind Sie längst Teil der Informationsgesellschaft des 21. Jahrhunderts!

Doch achten Sie auch immer ausreichend auf Ihre Online-Sicherheit?

Jede Internet-Nutzung birgt Risiken. So hinterlassen Sie im Netz wertvolle Daten, nutzen Online-Zahlungssysteme oder schließen per eMail Verträge.

Diese Broschüre soll Ihnen mit Informationen rund um Viren, Cookies, Datenschutz und Gütesiegel sowie mit vielen weiteren Aspekten einen Überblick geben über die rechtlichen Grundlagen einerseits und zahlreiche praktische Lösungsansätze andererseits.

Sicher Surfen

1 Grundregeln für sicheres Surfen

Diese Checkliste soll Ihnen helfen, eventuelle Fallen zu umgehen.

- Speichern Sie auf Ihrem Rechner niemals sensible Daten, wie z.B. Passwörter, Bank- oder Kreditkartendaten!

- Versenden Sie diese Daten niemals per eMail, denn unverschlüsselte Daten können ohne weiteres abgefangen werden.

- Sorgen Sie für Ihren PC mit Internetzugang für ein Virenschutzprogramm, das sich zudem regelmäßig aktualisiert. Sie können nur dann auf Virenschutz verzichten, wenn Sie ein nicht virenanfälliges Betriebssystem nutzen.

- Schützen Sie sich vor SPAM. Geben Sie Ihre eMail-Adresse so selten wie möglich heraus. Weiteren Rat zum Schutz vor SPAM bekommen Sie auf unserer Internetseite www.ecommerce-verbindungsstelle.de unter „Tipps“ sowie unter www.verbraucher-gegen-spam.de.

- Öffnen Sie keine eMails von unbekannten Absendern und öffnen Sie keine fragwürdigen Dateianhänge - sie könnten mit Viren infiziert sein.

- Glauben Sie keinen Gewinnversprechen, wenn Sie nicht an einem Gewinnspiel teilgenommen haben. Niemand verschenkt einfach so Geld! Dasselbe gilt für dubiose Erbschaften oder angeblich auf den Bankkonten vergessenes Geld früherer afrikanischer Diktatoren. Mehr Informationen hierzu finden Sie auch auf unserer Internetseite www.ecommerce-

verbindungsstelle.de in der Rubrik „Vorsicht Falle“ unter den Stichworten „Nigeria-Connection“ und „Gewinnversprechen.“

- Bevor Sie auf einer Internetseite Ihren Namen und Ihre eMail-Adresse angeben, prüfen Sie genau, ob Sie nicht gerade im Begriff sind, einen kostenpflichtigen Vertrag oder ein Abonnement abzuschließen. Schon viele Verbraucher haben „aus Versehen“ eine Bestellung abgeschickt. Mehr Informationen zur „Abo-Falle“ bekommen Sie auch auf unserer Internetseite unter www.ecommerce-verbindungsstelle.de.

- Wenn Sie im Internet einkaufen, überprüfen Sie zuvor stets den Anbieter. Ist er leicht zu erreichen (eMail, Telefon, vollständige Adresse angegeben)? Rufen Sie den Verkäufer ruhig einmal an und stellen Sie einige Fragen zum Produkt. So gewinnen Sie einen persönlichen Eindruck. Mehr Informationen zum Online-Einkauf bieten das Merkblatt „Online-Einkauf? Aber sicher!“ und die Broschüre „Shopping Online“ auf unserer Internetseite unter www.ecommerce-verbindungsstelle.de .

- Lesen Sie, wie der Verkäufer bewertet wurde, wenn Sie an einer Onlineauktion teilnehmen: Wurde er in letzter Zeit oft negativ bewertet, oder ist dies sein erster Verkauf überhaupt? Dann sollten Sie sehr vorsichtig sein und wenn überhaupt nur für kleinere Geldbeträge einkaufen. Beachten Sie aber, dass auch eine positive Bewertung keine absolute Sicherheit bietet.

- Achten Sie auf Gütesiegel! In Deutschland gibt es verschiedene Anbieter von Gütesiegeln, die Internetshops auszeichnen. Mehr Informationen hierzu in Kapitel 4 der Broschüre.

- Überweisen Sie auf keinen Fall größere Beträge ohne Absicherung! Mehr Informationen zu verschiedenen Zahlungssystemen in Kapitel 3 dieser Broschüre.

2 Virenschutz

Internetviren sind die Krankheitskeime einer technisierten Gesellschaft. Es handelt sich bei Viren um kleine Programme, deren einziger Zweck darin liegt, fremde Computer zu infizieren und zu schädigen. Mit der Verbreitung des Internet haben sich zudem neue „Schädlinge“ entwickelt: „Würmer“ verbreiten sich über eMails und suchen nach Sicherheitslücken des Rechners. Die gefährlichste Variante ist wohl der „Trojaner“, der den Computer nach außen öffnet, so dass der Erschaffer des Trojaners den infizierten Rechner beherrschen kann. Ihre Daten könnten abgelesen werden, Ihr Rechner könnte als Absender von SPAM und als Lagerplatz für illegale Software genutzt werden.

Doch Sie können sich gegen solche Gefahren effektiv durch die Auswahl eines nicht virenanfälligen Betriebssystems oder durch die Installation eines Virenschutzprogramms zur Wehr setzen. Da sich Computerviren wie echte Viren weiterentwickeln, sollten Sie auch regelmäßig für eine Aktualisierung Ihres Virenschutzes sorgen. Die entsprechende Software finden Sie im Internet.

Zudem sollten Sie insbesondere mit dem eMail-Programm virenanfälliger Betriebssysteme keine unbekannten eMails oder Anhänge öffnen. Bevor Sie Anhänge öffnen, sollten Sie diese zuvor auf Viren untersuchen. Besonders bei den Anhängen mit den Dateitypen .exe, .bat, .com und .vbs sollten Sie vorsichtig sein. Auch das Vorschaufenster Ihres eMail-Programms ist ein zusätzliches Sicherheitsrisiko, da diese kleine Lücke einigen Schädlingen bereits genügt, um sich auf Ihrer Festplatte festzusetzen. Als „Notfallkoffer“ sollten Sie stets eine Startdiskette oder CD-ROM mit den von Ihnen genutzten Programmen bereithalten. Diese erhalten Sie entweder mit Ihrem Antivirenprogramm oder Sie können sie selbst erstellen.

Interessante Links zum Thema Viren:

www.antivirus-online.de – IT-Security Portal
www.av-test.de – AV Test GmbH
http://www.heise.de/security/ **-** heise Security

3 Bezahlen im Internet

Wird ein Geschäft über das Internet abgeschlossen, so wirft die Frage der Bezahlung nicht selten Probleme auf. Einerseits soll der Vertrag möglichst ebenso schnell und einfach abgewickelt werden wie ein Einkauf in einem Ladengeschäft. Andererseits sollen sich beide Vertragspartner auf eine ordentliche und sichere Durchführung des Bezahlvorgangs verlassen können.

Neben herkömmlichen Zahlungsarten, wie z.B. der Zahlung per Überweisung, Kreditkarte und Nachname, wurden zwischenzeitlich Systeme für die Zahlung über das Internet eingerichtet. Wenn Sie hierbei einige Vorsichtsmaßnahmen beachten, sind Sie beim bargeldlosen Bezahlen im Zeitalter des Internet auf der sicheren Seite.

Frage 1 **- Was sollte ich generell bei Zahlungen im Internet beachten?**

- Als Käufer steht Ihnen grundsätzlich nicht das Recht zu, die Zahlungsart zu bestimmen. Oft können Sie aber zwischen verschiedenen Zahlungsmöglichkeiten wählen, die Ihnen der Unternehmer auf seiner Internetseite anbietet, oder Sie können sich mit dem Verkäufer auf eine Zahlungsart verständigen, mit der beide Seiten einverstanden sind. Die Zahlungsbedingungen (auch anfallende Gebühren) sollten

Sie vor der Bestellung genau klären, damit Sie hinterher keine unangenehmen Überraschungen erleben.

- Bei Vorauszahlungen - per Kreditkarte, Scheck oder Überweisung - sollten Sie sich zuvor besonders gut über Ihren Vertragspartner informieren, um nicht an einen Betrüger zu geraten. Erkundigen Sie sich auch (z.B. bei Ihrer Bank), wie Sie Ihre Zahlung absichern und unter welchen Bedingungen Sie eine Zahlung auch nachträglich widerrufen können. Ohne sich abzusichern, sollten Sie niemals größere Summen überweisen!
- Zu einer rechtzeitigen Zahlung des Kaufpreises sind Sie auf jeden Fall verpflichtet. Behauptet der Verkäufer, dass eine Zahlung gar nicht oder nicht rechtzeitig eingetroffen sei, sind Sie beweispflichtig dafür, dass Sie den Geldbetrag rechtzeitig überwiesen haben. Sie sollten deshalb Kontoauszüge, Quittungen und Überweisungsbelege über die von Ihnen geleisteten Zahlungen unbedingt aufheben.
- Wenn Sie nicht rechtzeitig bezahlen, kann der Verkäufer von Ihnen unter Umständen Mahngebühren und Verzugszinsen verlangen. Er wird Sie an die Zahlung erinnern und kann, wenn Sie darauf nicht reagieren, einen Mahnbescheid beantragen. Schlimmstenfalls kann es zu einer Zwangsvollstreckung kommen.
- Der Verkäufer wird sich in seinen AGB meist das Eigentum bis zur vollständigen Bezahlung des Kaufpreises vorbehalten. Dies bedeutet, dass Sie die Ware zwar sofort nutzen können, die Ware aber erst mit der Zahlung des vollen Kaufpreises auch sicher behalten dürfen.
- Weitere Hinweise zur Sicherheit beim Online-Banking und zum eCommerce als Bankdienstleistung bietet der Bundesverband der deutschen Banken unter www.bdb.de.

Frage 2 - Welche Internet-Zahlungssysteme kann ich nutzen?

Die speziell für das Internet entwickelten Zahlungssysteme konnten sich nur begrenzt durchsetzen, zum Teil wurden die Angebote auch mangels Nachfrage wieder eingestellt. Drei unterschiedliche Ansätze für die bargeldlose Zahlung im Internet lassen sich herauskristallisieren:

Die Guthabenkarten (Prepaidkarten)

Die Guthabenkarten fürs Internet funktionieren ähnlich wie Guthabenkarten für Handys: Der Kunde kauft etwa an einer Tankstelle oder an einem Kiosk eine Karte in Höhe eines bestimmten Einkaufswertes und kann mit Hilfe dieser Karte im Internet anonym einkaufen. Unter Angabe des Namens der Karte, mit einem PIN-Code und einem Passwort kann er bezahlen. Der Betrag wird daraufhin von seinem Kartenguthaben abgebucht.

Die **„Paysafecard“**, die es außer an Tankstellen und Kiosken in Tabakgeschäften oder Filialen des Bertelsmann Clubs gibt, ist im Wert von 10, 25, 50 oder 100 € erhältlich. Die Zahlung mit dieser Karte wird von ungefähr 2000 Anbietern akzeptiert.

Die „**MicroMoney“- Karte** ist ein Produkt der Deutschen Telekom, die vor allem für die Zahlung kleinerer Beträge im Internet angeboten wird. Die Karten mit einem Guthaben von 15 € gibt es in jedem T-Punkt. Die Guthabenkarten können Sie auch online erwerben zu 15, 30 oder 50 €. Näheres unter: www.paysafecard.com und www.micromoney.de.

Mobile Payments

Zu den neueren Zahlungsverfahren gehören auch die so genannten „Mobile Payments“, die oft das (Mobil-)Telefon in den Zahlungsvorgang einbeziehen. Doch inzwischen haben einige Anbieter, wie z.B. Streetcash, Paybox oder Payitmobile ihre Angebote für den Endkunden auf dem deutschen Markt wieder eingestellt. Vodafone bietet für Unternehmer das mobile Bezahlverfahren m-pay an, dabei übernimmt Vodafone die Abrechnung mit dem Endkunden. T-Pay, die Bezahlplattform der Deutschen Telekom, bietet neben dem bereits oben geschilderten „MicroMoney“ auch die Varianten „Call and Pay“ oder „T-Com Rechnung“ an.

Dieses Zahlungsverfahren basiert auf der Idee, dass der Kunde stets mobil mit seinem Telefon zahlen kann. Das Telefon wird dazu eingesetzt, eine weitere „Sicherung“ in das Verfahren einzubauen. Entweder tippt der Kunde auf der entsprechenden Seite des Händlers seine Mobilfunknummer ein und muss die Zahlung später per SMS mit seiner persönlichen Identifikationsnummer (PIN-Code) bestätigen oder er ruft eine kostenlose Telefonnummer zur Bestätigung seines Einkaufs an. Näheres unter www.vodafone.de und www.t-pay.de.

Elektronisches Geld: eCash / CyberCoins

Unter diesen Namen wurden Verfahren zur Bezahlung mit elektronischem Geld eingeführt. Ähnlich der Bezahlung mit einer Geldkarte buchte der Kunde einen bestimmten Geldbetrag von seinem Konto ab und speicherte diesen auf seinem Rechner. Mit diesem virtuellen Geld konnte er im Internet Einkäufe vornehmen. Dieses Zahlungsmittel sollte es ermöglichen, Online-Geschäfte jeglichen Umfanges sicher zu tätigen. Nach den uns vorliegenden Informationen wurden jedoch derzeit in Deutschland alle Projekte zu diesem Zahlungsverfahren eingestellt.

Frage 3 - **Wie kann ich meine Zahlungen absichern?**

Ihre Zahlungen sollten Sie im Hinblick auf zwei mögliche Risiken absichern: Zum einen könnte bei Online-Zahlungen ein Dritter Ihre Daten ausspähen und missbrauchen. Zum anderen könnte der Verkäufer das Geld einfach einstecken und verschwinden.

Wenn eine Zahlung auf Rechnung oder per Nachnahme nicht möglich ist, sollte auf andere Sicherungen oder Treuhandsysteme zurückgegriffen werden.

- **Online-Bezahlsysteme**

Online-Bezahlsysteme haben den Vorteil, dass Geld schnell und unkompliziert auf dem gesamten Globus übertragen werden kann, ohne dass dafür Bank- bzw. Kreditkartendaten an den Verkäufer übermittelt werden. Manche Anbieter solcher Systeme verlangen vom Kunden ebenfalls, dass er in Vorleistung geht, indem er Guthabenkarten erwirbt. Es gibt jedoch auch Systeme, die die Zahlung per Kreditkarte oder per Lastschriftverfahren erst bei oder nach dem Versand der Ware verlangen. Ihr Vorteil liegt darin, dass Ihre sensiblen Daten zur Bankverbindung oder Kreditkarte nur dem Unternehmen des Online-Bezahlsystems bekannt sind, jedoch gerade nicht an den unbekannten Verkäufer übermittelt werden.

Das System kann zusätzlich einen Käuferschutz beinhalten, dies umfasst eine durch einen Selbstbehalt begrenzte Absicherung des Käufers für den Fall der Nichtlieferung der Ware. Ob ein Käuferschutz geleistet wird und unter welchen Bedingungen Geld erstattet wird, sollten Sie unbedingt vor der Auswahl des Systems überprüfen.

Online-Bezahlsysteme sind Paypal, Web.Cent, Moneybookers, Firstgate Click&Buy, Clickpay, T-Pay oder Paysafecard, um nur einige Unternehmen beispielhaft zu nennen.

- **Treuhänder ("escrow service")**

Bei Einsatz eines Treuhänders wird der Geldtransfer „zu treuen Händen“ über einen Dritten abgewickelt. Dieser Dritte soll sicherstellen, dass das Geld erst dann an den Verkäufer ausgezahlt wird, wenn die Ware angekommen und in Ordnung ist. Umgekehrt wird der Verkäufer vor unberechtigten Rückbuchungen durch den Käufer geschützt. Für diesen Service fällt eine bestimmte Gebühr an. Klassische Treuhänder sind Notare, Rechtsanwälte oder auch Banken, doch mit der Entwicklung des Internet und der Zunahme von grenzüberschreitenden Geschäften entstand der Bedarf nach einem internationalen Treuhandverfahren, das entsprechend automatisiert ist. Bekannte und von Ebay empfohlene Online-Treuhänder sind z.B. iloxx.de, Safe Trade, Escrow Europa oder Triple Deal.

Allerdings gibt es auch betrügerische Treuhandfirmen, die das Sicherheitsbedürfnis der Kunden ausnutzen.

Daher sollten Sie bei der Auswahl des Treuhandservice stets die folgenden Tipps beachten:

- Nutzen Sie bei Auktionen nur den von dem Auktionshaus angegebenen Treuhandservice.
- Seien Sie misstrauisch, wenn Ihr Verkäufer auf einen bestimmten Treuhänder besteht. Bedauerlicherweise gibt es „Online-Treuhänder“, die nur für wenige Wochen gegründet werden und mit Anbietern von Waren zusammenarbeiten, um Käufer zu prellen.
- In den Diskussionsforen der Auktionshäuser können Sie sich informieren, ob der Treuhänder bereits negativ aufgefallen ist!
- Überprüfen Sie Adresse und Telefonnummer des Treuhänders und schauen Sie nach Gütesiegeln. Kontrollieren Sie auch, wer als Domaininhaber eingetragen ist und wie lange diese Seite schon so existiert.

Informationen dazu finden Sie unter der Seite der Registrierungsstelle für „.de“-Domains www.denic.de und für alle anderen Domains unter http://www.whois.net/.

- Rufen Sie den Treuhänder ruhig vorab an und stellen Sie Fragen zum Service. Wenn offizielle Stellen, Banken oder Gütesiegelvergabestellen als Partner angegeben werden, überprüfen Sie vorab die angegebenen Telefonnummern, und fragen Sie dort telefonisch nach.
- Natürlich können auch Sie dem Verkäufer zur Abwicklung des Kaufs einen Treuhänder vorschlagen. So können Sie auf bekannte Online-Treuhänder zurückgreifen. Erkundigen Sie sich bei Banken, Rechtsanwälten und Notaren nach entsprechenden Service-Angeboten. Zumindest bei rein nationalen Geschäften wird Ihr Vertragspartner die Vertrauenswürdigkeit dieses Treuhänders richtig einschätzen können und Ihren Vorschlag akzeptieren.
- Beachten Sie, dass die Western Union Bank kein Treuhandverfahren anbietet. Zahlungen über die Western Union Bank können binnen weniger Minuten im Zielland abgehoben werden. Dafür muss der Empfänger nur seinen Personalausweis vorlegen. Mit der Person verliert sich dann auch die Spur Ihres Geldes.

Interessante Links zum Thema Zahlungsarten im Internet:

www.begin.de – E-Commerce-Beratungszentrum der IHK Hannover
http://pages.ebay.de/help/index.html - Ebay Informationen zu Zahlungsarten
www.verbraucherzentralen.de – Die Verbraucherzentralen in Deutschland
www.bdb.de – Bundesverband Deutscher Banken

4 Gütesiegel für Internetshops

„Aus Schaden wird man klug?“ Wer bereits ein Mal negative Erfahrungen gemacht hat, wird vorsichtiger bei Einkäufen im Internet. Woran kann man sich bei Einkäufen im Internet orientieren? Gibt es keine verlässlichere Alternative zu Diskussionsforen oder individuellen Käufer-Bewertungen? Um das Vertrauen in den Online-Handel zu stärken, wurden auch für das Internet Gütesiegel entwickelt, die bereits in anderen Bereichen der Wirtschaft ein Hinweis auf die Qualität des Produkts sind.

Leider wurde bisher noch kein einheitliches Gütesiegel für den Online-Handel geschaffen. Einige Gütesiegel prüfen zum Teil nur die Identität des Unternehmens, andere Gütesiegel beinhalten eine „Geld-zurück-Garantie“ für den Käufer. Angesichts der Vielfalt der Anbieter, ihrer verschiedenen Leistungen und auch der unterschiedlichen Qualität, drohte nicht nur das Vertrauen in den Online-Handel, sondern auch in die Gütesiegel an sich zu schwinden.

Um dem entgegenzuwirken, hat die **Initiative D21** der deutschen Wirtschaft (www.internet-guetesiegel.de) eine Anzahl von Qualitätskriterien für Online-Angebote entwickelt. Gütesiegelanbieter, die verbindlich erklärt haben, dass sie diese Kriterien einhalten werden, wurden von der Initiative D21 in eine Empfehlungsliste aufgenommen. Es handelt sich um die folgenden Gütesiegel: Trusted shops, TÜV safer shopping, ips internet privacy standards und „EHI geprüfter Online Shop“ (mit Eurolabel) und „EHI“ (mit dem Label des Bundesverbandes des deutschen Versandhandels).

Sicher Surfen

Frage 1 - **Wie erhält ein Shop ein Gütesiegel?**

Wenn sich ein Anbieter um ein Gütesiegel für sein Internet-Angebot bewirbt, so wird sein Unternehmen zunächst genau geprüft. Von der korrekten Anwendung der gesetzlichen Vorschriften (z.B. des Fernabsatzgesetzes für den Verbrauchsgüterkauf), über die Regelungen des Datenschutzes bis hin zur organisatorischen und finanziellen Sicherheit des Unternehmens und der Benutzerfreundlichkeit des Angebots reicht der Katalog der überprüften Kriterien. Natürlich erfolgt diese Prüfung nicht kostenlos: Zwischen 250 € und 50 000 € für die meist jährlichen Kontrollen verlangen die Prüfungsinstitute, je nach Umfang der Untersuchung. Nur wenn das Unternehmen alle Anforderungen erfüllt, darf es das begehrte Gütesiegel auf seiner Homepage verwenden.

Frage 2 - **Welche Vorteile bieten Gütesiegel den Käufern?**

Der Käufer kann sich darauf verlassen, dass ein Unternehmen, das ein Gütesiegel trägt, z.B. die Datenschutzgesetze und Informationspflichten einhält. Auf der Internetseite des Gütesiegelanbieters kann sich der Käufer über den Umfang der erfüllten Kriterien informieren, sowie auch darüber, ob damit eine Geld-zurück-Garantie oder andere Leistungen verbunden sind. Zudem kann er schlechte Erfahrungen mit einem geprüften Unternehmen auch direkt dem Gütesiegelanbieter melden.

Frage 3 - **Was sind die Vorteile für den Verkäufer?**

Durch das Gütesiegel können Verkäufer auf einen bedeutenden Vertrauensbonus bei den Käufern setzen. Das Gütesiegel kann als Marketingelement genutzt werden, um neue Kunden anzuwerben. Viele Unternehmen berichten von Umsatzsteigerungen nach der Einrichtung eines Gütesiegels auf ihrer Homepage. Zudem profitieren sie von der Überprüfung der Gütesiegelvergabestelle,

denn diese kontrolliert die Allgemeinen Geschäftsbedingungen und die Einhaltung von verbraucher- und datenschutzrechtlichen Bestimmungen.

Interessante Links zum Thema Gütesiegel:

www.internet-guetesiegel.de - Projekt der Initiative D21
www.trustedshops.de - Trusted Shops Gütesiegel
www.safer-shopping.de - S@fer Shopping - TÜV geprüft
www.datenschutz-nord.de - Datenschutz Nord GmbH Landesgesellschaft der Freien Hansestadt Bremen
www.shopinfo.net - EHI- Online Einkaufen mit Vertrauen

5 Elektronische Signatur

Wer im Internet einen Vertrag abschließt, benutzt dafür üblicherweise auch die Kommunikationsformen, die das Internet bietet. Der Vertragsabschluss erfolgt daher z.B. durch die Eingabe einer Bestellung mit dem abschließendem Klick auf den Button „Bestellung abschicken“ oder durch den Austausch von eMails mit dem Vertragspartner.

Diese Art des Vertragsabschlusses birgt aber das Risiko, dass die online übertragenen Daten durch den Zugriff eines unbefugten Dritten gelesen und sogar verändert werden können, ohne dass die Vertragsparteien dies erkennen könnten.

Zudem ist Folgendes zu beachten: Kommt es später zu Streitigkeiten über das online abgeschlossene Geschäft, so haben die ausgedruckten eMails oder Bestellformulare nur eine geringe Beweiskraft: Da diese Dokumente weder eine handschriftliche Unterschrift noch ein Siegel tragen, besitzen sie nicht die Eigenschaften einer Urkunde und ihr Beweiswert vor Gericht ist gering. Das Gericht nimmt diese Dokumente im Rahmen des Verfahrens lediglich in Augenschein.

Nach der Einführung neuer Vorschriften zu elektronischen Signaturen in das deutsche Recht steht Anbietern und Nutzern in Deutschland nunmehr ein rechtlich anerkanntes elektronisches System zur Verfügung, mit dem vertrauliche Inhalte sicher und ohne unbemerkte Veränderungen transportiert werden können.

Denn elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, wurden in ihrer Beweiskraft Urkunden gleichgestellt (§ 371 a ZPO).

Frage 1 - **Ist die elektronische Signatur so gut wie ein schriftlicher Vertrag?**

Obwohl für die meisten Rechtsgeschäfte keine Verpflichtung besteht, eine bestimmte Form einzuhalten, so dass fast alle Verträge auch mündlich, per Telefon oder per Internet abgeschlossen werden können, hat der Gesetzgeber für bestimmte Geschäfte die **Schriftform** (z.B. die Bürgschaftserklärung) oder sogar die notarielle Beurkundung (z.B. Verträge über Grundstücke) vorgeschrieben.

Der Schriftform genügte nach alter Rechtslage die elektronisch oder digital signierte Erklärung nicht.

Zur Förderung des elektronischen Handels wurde indes eine neue Bestimmung in das Bürgerliche Gesetzbuch eingefügt (§ 126 Abs. 3 BGB), wonach die schriftliche Form durch die elektronische Form ersetzt werden kann, sofern nicht durch das Gesetz etwas anderes bestimmt ist. Die elektronische Form ist also eine Variante der **Schriftform** mit fast derselben Qualität. Die elektronische Form hat nach § 126 a BGB ein elektronisches Dokument immer dann, wenn es mit einer **qualifizierten** elektronischen Signatur nach dem Signaturgesetz versehen ist. Die elektronische Form ist nur dort nicht ausreichend, wo sie im Gesetz ausdrücklich ausgeschlossen wird, z.B. bei Kündigung eines Arbeitsvertrages oder bei Abschluss eines Verbraucherkreditvertrages.

Andererseits reicht für einige Erklärungen - etwa die Betriebskostenabrechnung im Mietrecht - auch die in § 126 b BGB definierte **Textform**: eine lesbare, aber unterschriftslose Erklärung, bei der der Erklärende durch Nachbildung der Namensunterschrift oder anders erkennbar gemacht wird (z.B. ein Computer-Fax oder eine eMail mit eingescannter Unterschrift).

Frage 2 – **Welche Signaturverfahren gibt es?**

Das neue Signaturgesetz definiert in § 2 SigG drei verschiedene Verfahren: die elektronische, die fortgeschrittene elektronische und die qualifizierte elektronische Signatur.

Die „**einfache**“ elektronische Signatur besteht in der Beifügung von Daten, die der Authentifizierung des Absenders dienen. Dies kann z.B. durch eine eingescannte Unterschrift des Absenders geschehen.

Die **fortgeschrittene** elektronische Signatur beruht auf der so genannten asymmetrischen Verschlüsselungstechnik: Dabei werden ein geheimer, privater Schlüssel (private key) und ein öffentlich zugänglicher Schlüssel (public key) verwendet.

Der Absender der Nachricht schließt diese mit seinem privaten Schlüssel ab und der Empfänger kann die Signatur mit Hilfe des „öffentlichen“ Schlüssels aufschließen. Nach der Signierung eines Textes ist keine unbemerkte Veränderung mehr möglich. Jedem privaten Schlüssel ist genau ein einziger öffentlicher Schlüssel ausschließlich zugeordnet.

Der Empfänger der signierten Nachricht berechnet mit Hilfe einer Spezialsoftware eine Prüfsumme („Hashwert“) des als Text empfangenen Dokuments. Mit dem frei zugänglichen öffentlichen Schlüssel entziffert er daraufhin die Signatur des Absenders, die ebenfalls in einer bestimmten Prüfsumme besteht. Sind die beiden Summen identisch, so ist sicher, dass der Text mit dem Schlüssel des Absenders signiert und seitdem nicht verändert wurde. Daneben besteht die Möglichkeit, den Text vor dem Absenden so zu verschlüsseln, dass er nur von einem bestimmten Empfänger gelesen werden kann. Auch für diese zusätzliche Verschlüsselung des Textes wird die so genannte asymmetrische Verschlüsselungstechnik verwendet, wobei der öffentliche Schlüssel dann nicht frei zugänglich ist, sondern ausschließlich dem

Empfänger der Nachricht verfügbar gemacht wird. Dieses Verfahren der fortgeschrittenen elektronischen Signatur bietet hinreichende Sicherheit; natürlich nur solange der private Schlüssel dem unbefugten Zugriff entzogen ist.

Das Verfahren der **qualifizierten** elektronischen Signatur entspricht im Wesentlichen dem der fortgeschrittenen elektronischen Signatur. Der entscheidende Unterschied besteht darin, dass nur Schlüsselpaare verwendet werden, die von einem Zertifizierungsanbieter im Sinne von § 4 SigG herausgegeben wurden. Zudem befindet sich der private Schlüssel einer qualifizierten elektronischen Signatur auf einer externen Hardware (z.B. Chipkarte) und sollte so gesichert sein, dass er auch mit großem Aufwand nicht ausgelesen werden kann. Demgegenüber befinden sich bei der fortgeschrittenen elektronischen Signatur beide Teile eines Schlüsselpaares auf der Festplatte des Benutzers und könnten daher durch Zugriff von „Hackern“ ausgespäht werden.

Die Zuverlässigkeit dieser qualifizierten digitalen Signatur hängt wiederum von der Verlässlichkeit der Zertifizierungsanbieter ab. Diese können ihre Dienste seit Inkrafttreten des Signaturgesetzes in seiner neuen Fassung genehmigungsfrei betreiben. Sofern sie einen Sitz in Deutschland haben, müssen sie die Tätigkeit allerdings gegenüber der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen anzeigen. Letztere ist auch für die Durchführung des Signaturgesetzes verantwortlich und wacht über eventuelle Missbräuche.

Ein Zertifizierungsanbieter kann sich in Deutschland auch freiwillig akkreditieren lassen. Einem akkreditierten Zertifizierungsanbieter wird von der zuständigen Behörde ein Gütezeichen erteilt, als Nachweis einer umfassend geprüften technischen und administrativen Sicherheit der qualifizierten elektronischen Signaturen.

Sicher Surfen

Interessante Links zum Thema elektronische Signatur:

unter http://www.bundesnetzagentur.de erhalten Sie einen Überblick über die bisher zur Verfügung stehenden akkreditierten **Zertifizierungsdienste**

www.sicher-im-netz.de – Initiative von Politik und Wirtschaft für mehr Online-Sicherheit

www.siglab.de – Verein zur Förderung der elektronischen Signatur

6 Datenschutz

Das Internet ist von Natur aus auf den Austausch von Daten ausgerichtet. Mit jeder Mail, jedem Aufruf einer Homepage werden viele Informationen zwischen Anbieter und Nutzer ausgetauscht. Diese Daten haben sich in der Informationsgesellschaft bereits zu einem lukrativen Handelsgut entwickelt. Fühlen Sie sich bereits als „gläserner Verbraucher“? Oder glauben Sie noch an die Anonymität des Netzes? Welche Daten darf der Betreiber eines Onlineshops eigentlich sammeln, verarbeiten und weiterleiten? Zu diesem Thema finden Sie mehr Informationen auf den nun folgenden Seiten.

Frage 1 - **Was erfasst der Datenschutz inhaltlich?**

Dem gesetzlichen Datenschutz unterliegen grundsätzlich nur **personenbezogene** Daten. Geschützt werden daher Informationen über Einzelpersonen. Von den datenschutzrechtlichen Vorschriften werden alle Informationen erfasst, die über den Betreffenden Auskunft geben, insbesondere Name, Anschrift, Telefonnummer, Alter, Staatsangehörigkeit, Beruf.

Von den datenschutzrechtlichen Vorschriften werden alle Verarbeitungsphasen erfasst: So beginnt der Schutz bereits bei der Erhebung und erstreckt sich über die Speicherung, Veränderung, Übermittlung, Sperrung bis hin zur Löschung der Daten.

Frage 2 - **Welche rechtlichen Anforderungen bestehen für die Anbieter?**

Die Erhebung und Nutzung von personenbezogenen Daten ist nach deutschem Recht nur zulässig, wenn sie **gesetzlich gestattet**

wurde oder eine **ausdrückliche Einwilligung** des Betroffenen hinsichtlich der Verarbeitung vorliegt. Grundsätzlich sollen so wenige Daten wie möglich erhoben, verarbeitet und genutzt werden. Sobald der Diensteanbieter erfasste Daten nicht mehr benötigt, muss er sie löschen.

Der Anbieter muss

- den Nutzer über die Verwendung seiner personenbezogenen Daten und eventuelle Widerspruchsrechte unterrichten,
- in bestimmten Fällen eine Einwilligung des Nutzers einholen und
- bei der Erstellung von pseudonymen Nutzerprofilen und der Verwendung von Cookies besondere Regeln beachten.

Frage 3 - **Worüber muss der Internetnutzer unterrichtet werden?**

Zu Beginn eines Nutzungsvorganges ist der Betroffene stets nach § 4 Abs. 1 TDDSG (Teledienstedatenschutzgesetz) über Art, Umfang und Zweck der Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten zu informieren. Insbesondere auf eine mögliche Verarbeitung außerhalb des europäischen Wirtschaftsraumes muss er gesondert hingewiesen werden. Außerdem ist der Anbieter verpflichtet, den Nutzer über sein eventuelles Recht auf Berichtigung, Sperrung oder Löschung seiner personenbezogenen Daten hinzuweisen. Darüber hinaus hat der Nutzer auch bei nur kurzfristiger Speicherung das Recht, die zu seiner Person gespeicherten Daten unentgeltlich (u. U. elektronisch) einzusehen.

Frage 4 - **Wann muss die Belehrung erfolgen?**

Die Unterrichtung sollte spätestens erfolgen, wenn der Nutzer zur Angabe persönlicher Daten aufgefordert wird, oder wenn Dateien mit direktem oder indirektem Personenbezug von seinem Rechner abgerufen werden sollen (z. B. in Cookies, hierzu unten).

Frage 5 - **In welcher Form sollte die Belehrung erfolgen?**

Der Hinweis auf die Unterrichtung muss so platziert werden, dass ein Nutzer sie üblicherweise zur Kenntnis nimmt, sobald er das betreffende Angebot aufruft. Sie muss insbesondere

- in ausreichend großer Schrift erfolgen,
- für den Nutzer jederzeit abrufbar sein,
- im oberen, sichtbaren Teil untergebracht werden und zwar so, dass der Bildschirminhalt nicht durch Scrollen verschoben werden muss,
- möglichst auffällig gestaltet, also hervorgehoben sein.

Der Hinweis kann unmittelbar auf der Startseite stehen oder über einen Link von der Start- bzw. Bestellseite erfolgen. Alternativ kann, bevor ein ausgefülltes Formular elektronisch verschickt wird, die Unterrichtung in einem so genannten Pop-Up Fenster erfolgen, wobei eine ausdrückliche Abbruchmöglichkeit gegeben sein muss. Jedenfalls reicht weder die bloße Aufnahme der Datenschutzerklärung in die Allgemeinen Geschäftsbedingungen noch ein pauschaler Hinweis, dass dem Datenschutz Rechnung getragen werde.

Frage 6 - **Welche Regeln gelten für die Einwilligung?**

Wenn die Nutzung der Daten nicht bereits gesetzlich gestattet ist, benötigt der Anbieter die Einwilligung des Nutzers. Diese Einwilligung kann schriftlich und auf elektronischem Wege erfolgen. Zuvor muss der Nutzer über den beabsichtigten Verwendungszweck informiert werden.

Der Anbieter muss sicherstellen, dass die Einwilligung auf eine bewusste und eindeutige Handlung zurückzuführen ist und nicht etwa auf einem versehentlichen Mausklick beruht. Die Einwilligung muss vom Anbieter zudem protokolliert und so gespeichert werden, dass sie für den Nutzer jederzeit abrufbar ist.

Der Nutzer hat das Recht, diese Einwilligung jederzeit zu widerrufen. Auch auf dieses Recht muss er vor Erklärung seiner Einwilligung hingewiesen werden.

Frage 7 - **Was sind eigentlich „Cookies?“**

Bei den so genannten Cookies handelt es sich um Dateien, die ein Anbieter automatisch auf dem Rechner des Kunden anlegt, um sie jedes Mal dann aufzurufen, wenn der Kunde die Seite des Anbieters öffnet.

Datenschutzrechtlich problematisch sind diese Cookies, weil der Datenaustausch in aller Regel geschieht, ohne dass der Benutzer etwas davon bemerkt. Zudem kann der Anbieter auf diesem Wege Informationen über das Surfverhalten des Nutzers sammeln, ein Nutzerprofil entwickeln und dem Nutzer gezielt Angebote unterbreiten.

Ein Anbieter, der Cookies verwenden und anlegen möchte, muss daher den Nutzer genau über deren Zweck, Inhalt und Dauer der Datenverarbeitung informieren und per Mausklick sein

Einverständnis einholen. Auch diese Informationen sollten entweder bereits auf der Startseite hinterlegt oder über einen deutlich sichtbaren Link abrufbar sein.

Sicherheitsbewusste Internetnutzer können in ihrem Browser einstellen, inwieweit Cookies akzeptiert werden. Wer Cookies zulässt, sollte diese in regelmäßigen Abständen löschen.

Interessante Links zum Thema Datenschutz :

http://www.bfd.bund.de/ - Der Bundesbeauftragte für Datenschutz

http://www.datenschutz.de/ - Virtuelles Datenschutzbüro

http://www.datenschutzzentrum.de – Landeszentrum für Datenschutz Schleswig-Holstein

7 Das Internet als Spielplatz?

Das Surfen im Internet ist besonders bei Kindern und Jugendlichen beliebt. Die Eltern müssen sich bisweilen sorgenvoll mit vielen Fragen auseinandersetzen. Sind Kinder im Internet dort im Vergleich zu erwachsenen Nutzern nicht besonders gefährdet? Was passiert, wenn sie eigenständig etwas bestellen? Wie kann ich sie vor Gefahren schützen?

Frage 1 - Können Minderjährige im Internet eigentlich Verträge abschließen?

Für Geschäfte mit Minderjährigen gelten im Internet die gleichen Besonderheiten wie im "richtigen Leben" auch. Dabei wird zwischen Kindern unter sieben Jahren einerseits und Kindern und Jugendlichen zwischen sieben und 18 Jahren andererseits unterschieden.

Kinder unter sieben Jahren können rechtlich gesehen keine wirksame Willenserklärung abgeben und damit auch keine wirksamen Verträge abschließen.

Kinder und Jugendliche ab dem siebten und vor der Vollendung des 18. Lebensjahres sind „beschränkt geschäftsfähig“. Dies bedeutet, dass die Wirksamkeit des Vertrages von der Erlaubnis oder Genehmigung der gesetzlichen Vertreter abhängt. Eine Ausnahme hiervon sind Geschäfte, die ein Minderjähriger mit seinem Taschengeld eigenständig tätigen kann und nach der Zweckbestimmung durch seine Eltern auch darf. So ist z.B. der Kauf von Schokolade im Supermarkt auch ohne Zustimmung der Eltern möglich und wirksam. Denn die Schokolade wird sofort vom Taschengeld bezahlt, hier kann keine Überschuldung des

Minderjährigen eintreten. Minderjährige können sich dagegen nicht zu einem Abonnement oder zu einer Ratenzahlung verpflichten.

Frage 2 - Welchen Schutz gibt es vor jugendgefährdenden Inhalten im Netz?

Kinder und Jugendliche sollen vor Inhalten mit jugendgefährdendem pornographischem Inhalt geschützt werden. Die Anbieter solcher Seiten sind daher unter Androhung von Strafe verpflichtet, den Zugriff auf diese Seiten zu beschränken und diesen nur Erwachsenen zu gewähren.

Dies soll durch die Verwendung so genannter **Altersverifikationssysteme** (AVS) geschehen. Nach Ansicht der Kommission für Jugendmedienschutz bietet ein System nur dann hinreichende Sicherheit, wenn der Zutritt zu der geschlossenen Benutzergruppe über eine Volljährigkeitsprüfung erfolgt, die persönlichen Kontakt erfordert, so z.B. ein Post-Ident-Verfahren. Zweitens müsse auch bei jedem Bestellvorgang eine Authentifizierung erfolgen. Jedoch werden AVS zum Teil ohne persönlichen Kontakt verwendet, so z.B. durch die Abfrage von Personalausweis- oder Kreditkartennummern. Hier besteht das Risiko, dass ein AVS umgangen werden kann. Zudem sind ausländische Seiten mit pornographischem Inhalt oft ohne Beschränkungen abrufbar.

Insofern ist zusätzlicher Schutz immer dann erforderlich, wenn auch Kinder den Computer nutzen. Die Installation eines **Filterprogramms** sollte nicht fehlen. Filterprogramme blockieren entweder Internetseiten, die bestimmte Stichwörter enthalten oder verhindern den Zugang zu bestimmten auf einer „schwarzen Liste“ stehenden Seiten. Solche Filterprogramme können Sie im Netz kostenlos oder auch kostenpflichtig finden. Computerzeitschriften berichten immer wieder über die Qualität von Filterprogrammen und bieten zum Teil selbst Software an. Ferner verkaufen auch die

Sicher Surfen

Zugangsprovider (wie z.B. AOL, T-Online oder Arcor) Filterprogramme.

Doch können weder Zugangsbeschränkungen noch Filterprogramme einen umfassenden Schutz bieten. Zumal da der computerversierte Nachwuchs nicht selten ohne große Mühe Filterprogramme umgehen kann.

Die Kontrolle der Eltern kann also durch technische Vorkehrungen keinesfalls ersetzt werden! Schauen Sie daher Ihren Kindern immer wieder beim Surfen über die Schulter und reden Sie mit Ihren Kindern offen über die Gefahren des Internet. Suchen Sie mit Ihrem Kind gemeinsam nach interessanten Seiten und beobachten Sie das Verhalten Ihres Kindes vor allem in Chat – Räumen.

Interessante Links zum Thema Minderjährige und Internet:
www.polizei-beratung.de - Bundesweites Präventionsprogramm der Polizei
www.jugendschutz.net - Gemeinsame Stelle für den Jugendschutz aller Länder
www.bayern.jugendschutz.de - Aktion Jugendschutz Landesarbeitsstelle Bayern e.V.
www.blinde-kuh.de - Suchmaschine für Kinder mit Tipps für Eltern und Kinder
www.internet-abc.de - Internet-ABC e.V. Portal für Kinder und Eltern
www.klicksafe.de - Safer Internet Programm mit vielen Tipps für Kinder, Jugendliche, Eltern und Pädagogen

SICHER SURFEN

www.ecommerce-verbindungsstelle.de
bei
Euro-Info-Verbraucher e.V.

Ein unabhängiger deutsch-französischer Verein
im Dienste des europäischen Verbraucherschutzes

Rehfusplatz 11
77694 KEHL
Deutschland

Tel.: 07851 991 48 0
Fax: 07851 991 48 11
Mail: info@ecommerce-verbindungsstelle.de