



secure-it in NRW. Mehr Sicherheit beim Internet-Shopping. Eine Orientierungshilfe. Initiative »secure-it.nrw.2005«

| Inhalt

»secure-it.nrw.2005« für mehr Sicherheit im Internet	2
Worauf kommt es beim Internet-Shopping an?	3
Was leisten Gütesiegel?	10
Warum die Gütesiegel der Initiative D21?	11
Selbst sicherer im Internet	12
Stichwörter und Abkürzungen	14
Adressen und Informationen zum E-Commerce	18



| »secure-it.nrw.2005« für mehr Sicherheit im Internet

Wir wollen den elektronischen Handel fördern

Der elektronische Handel hat eine wichtige Aufgabe als Schrittmacher für Wachstum und Konjunktur. Immer mehr Menschen nutzen diese Chancen:

- > aktuelle Preisvergleiche zu treffen,
- > direkten Zugang zu Produkten zu finden,
- > Rabatte durch gemeinsamen Direkteinkauf zu nutzen,
- > niedrigere Preise zu zahlen.

Um die Chancen des Internets auszuschöpfen, müssen bei den Verbrauchern Unsicherheiten über rechtliche Bestimmungen und Ängste vor Betrug und Datenmissbrauch ausgeräumt werden.

Im Wege der Selbstregulierung sind deshalb Gütesiegel entstanden, die Ihnen mehr Sicherheit beim elektronischen Einkauf garantieren. Die Initiative D21 als Zusammenschluss führender Unternehmen der Informationsgesellschaft hat sich auf Mindeststandards bei Gütesiegeln verständigt.

Internet als Motor für Unternehmen

Das Internet: Unendliche Weiten – ökonomisch ungenutzte Möglichkeiten. Das Medium ist nicht nur interessant für Konsumenten, sondern auch für die Unternehmen. Bisher fehlte jedoch die Sicherheit, die für viele Verbraucherinnen und Verbraucher unerlässlich und für gute Geschäfte erforderlich ist. Vorhandene Sicherheitssysteme sind zu kompliziert oder noch zu teuer. Deshalb sind im elektronischen Handel Gütesiegel die erste Wahl.

Wir wollen, dass sich mehr Menschen trauen

Die Gesetzgebung der letzten Jahre hat dafür gesorgt, dass im elektronischen Handel gewisse Mindeststandards eingehalten werden. Es sind aber längst nicht alle berechtigten Vorbehalte gegen das Internet-Shopping überwunden.

Wir wollen junge Unternehmen und alteingesessene »gute Adressen« ermutigen, mit ihren Angeboten ins Inter-

net zu gehen. Sicherheit und Qualität bringen einen wichtigen Wettbewerbsvorteil, den immer mehr neue Anbieter nutzen. Unter sicheren und verlässlichen Bedingungen.

Wie erreichen Sie mehr Sicherheit?

Die Wirtschaft regelt rund um die »Initiative D21« selbst, wie mehr Sicherheit organisiert werden kann und überwacht dies durch anerkannte Unternehmen. Bisher haben sich neun Anbieter von Gütesiegeln auf Mindeststandards geeinigt, nach denen sie Internet-Shops und Unternehmen jeder Größe und Art prüfen bzw. auf die sie die Unternehmen verpflichten. Auf Grund dieser Prüfung wird ein Siegel auf Dauer oder für eine bestimmte Frist erteilt. Die Nutzer dieser Siegel verpflichten sich, hohe Standards einzuhalten. Ziel ist es, in einer gemeinsamen Anstrengung das Vertrauen der Verbraucher zu rechtfertigen, damit die Potentiale des E-Commerce sich voll entfalten können.



| Worauf kommt es beim Internet-Shopping an?

Eindeutig erkennbare Partner

Kundinnen und Kunden müssen wissen, mit wem sie es zu tun haben. Die Forderung nach eindeutiger Erkennbarkeit der Partner resultiert aus dem Teledienstegesetz. Gütesiegel sollen prüfen, ob Konformität mit diesem Gesetz besteht. Dabei wird von den Unternehmen gefordert:

- > den Namen und die Anschrift, unter der sie ihren Sitz haben und vor Gericht ladungsfähig sind,
- > neben einer E-Mail-Adresse auch eine Telefonnummer, unter der eine Kontaktaufnahme möglich ist,
- > die Nennung eines Vertretungsberechtigten bei juristischen Personen,
- > die Veröffentlichung eines Handelsregisterauszugs und der zuständigen Aufsichtsbehörde,
- > die Angabe einer Umsatzsteueridentifikationsnummer (falls vorhanden),
- > berufsspezifische Angabepflichten bei bestimmten Diensten von Berufsgruppen (Anwälten, Therapeuten etc.),

> ein leicht auffindbares und druckbares »Impressum«.

Kein Medium kann die Identität einer Ware oder eines Anbieters so perfekt verfälschen wie das Internet. Nicht immer geschieht dies in Betrugsabsicht: allein die Unvollständigkeit der Adresse und die Beschränkung auf die elektronische Post erhöhen Misstrauen und Geschäftsrisiko. Denn nach Untersuchungen werden mehr als 30 Prozent der Kaufvorgänge von den Kunden abgebrochen, weil sie unsicher über die Sicherheit des Geschäfts werden. Shops mit einem Gütesiegel werden aber nicht nur auf Richtigkeit und Vollständigkeit der Adresse geprüft, sondern auch auf Auffindbarkeit, leichte Verständlichkeit und Lesbarkeit.

Neues Recht: Aufklärung über kommerzielle Angebote

Werbende oder werbeähnliche elektronische Angebote wie etwa Preisnachlässe und Gewinnspiele müssen im Verbraucherinteresse nach § 7 Teledienstegesetz als solche klar erkennbar sein.

Bei Angebot zum Abschluss von Fernabsatzverträgen oder Fernunterricht bestehen nach dem neuen Zivilrecht noch weitergehende Informationspflichten (§ 312c BGB). Der Kunde muss Bescheid wissen über:

- > die einzelnen Schritte zum Vertragsabschluss,
- > den Speicherort des Vertragstextes,
- > die Möglichkeiten, Eingabefehler zu erkennen und zu berichtigen,
- > die Verhaltensregeln, denen sich der Anbieter unterwirft, und über die Möglichkeiten des Zugangs zu diesen Regeln.

Verbraucherinnen und Verbraucher sollen so besser vor undurchsichtigen Angeboten geschützt werden.

Klare Preise – klare Verhältnisse

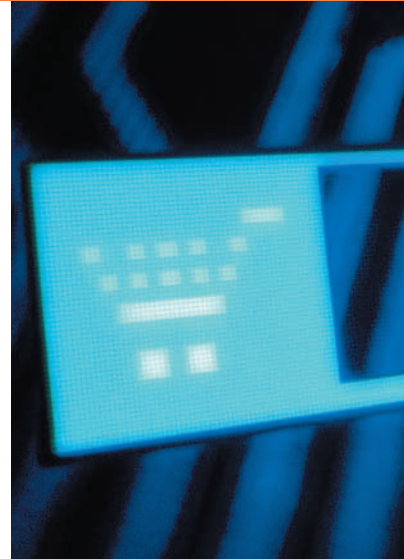
Bevor der Kunde verbindliche Bestellungen aufgibt, muss er informiert sein über:

- > Preise und Währung,
- > Nebenkosten und Steuern,
- > zusätzlichen Gebühren und Versandkosten.

Verschlüsselungstechniken:

SET (Secure Electronic Transaction) ist eine indirekte elektronische Zahlungsart, bei der Kunden und Shops sich einer Bank bedienen. Der Händler erhält eine Zahlungsgarantie, jedoch keine Kundendaten. Diese sind ausschließlich der Bank bekannt. SET erfordert eine Einrichtung auf dem Kunden-PC durch die Bank. Partner sind VISA, Mastercard, Microsoft, IBM u. a.

SSL (Secure Socket Layer) ist eine allgemeine Verschlüsselung der Kreditkartenbenutzung, die u. a. von Netscape angeboten wird. Darüber hinaus sind zahlreiche elektronische Zahlungssysteme am Markt und in Entwicklung.



Nicht nur auf der Ware, sondern auch im obligatorischen Warenkorb müssen alle Beträge erscheinen. Befristete Angebote müssen als solche kenntlich gemacht werden. In angemessenem Umfang soll über Zölle informiert werden. Auch auf die zusätzlichen Telekommunikationskosten für die Nutzung bestimmter Dienste muss deutlich hingewiesen werden.

Verständliche Abläufe

Die meisten Gütesiegel bieten nicht nur Sicherheit und klare Abläufe: Sie achten bei Anbietern auch auf Verständlichkeit und Bequemlichkeit des Internet-Auftritts und auf die »Software-Ergonomie« zugunsten der Kundinnen und Kunden. Diese Verständlichkeit zahlt sich für Käufer und Verkäufer aus.

Sie sollen jederzeit die einzelnen Schritte des Geschäfts erkennen!

Die grundlegenden Voraussetzungen eines Kaufvorgangs

> Der Kunde ist sich über den Kaufvorgang im Klaren und tätigt diesen nicht »nebenbei«.

- > Bis zum endgültigen Abschluss des Kaufvorgangs muss er jederzeit abzubrechen sein.
- > In der Endrechnung müssen alle Beträge und Nebenkosten enthalten sein.
- > Bei zeitgebundenen Bestellungen (Tagespreise) sollte beachtet werden, dass die Eingangsbestätigung durch den Anbieter auch über Zeitpunkt, Art und Umfang der Bestellung Auskunft gibt.
- > Beim Kaufvorgang im Internet spielt eine wichtige Rolle, dass die Käuferin oder der Käufer klar erkennen kann, wann der Kaufvorgang ausgelöst wird.
- > Ein ausdrückföhriger, rückverfolgbarer Nachweis (mit Auftragsnummer) ist das beste Mittel, um spätere Unklarheiten auszuschließen.
- > Nicht jeder Anbieter wird immer auch mögliche Zollgebühren angeben können, jedoch werden sich gute Shops darum bemühen.

Dies wird von allen Siegelanbietern im Rahmen der Softwareprüfung oder anhand von Testkäufen in den einzelnen Schritten nachvollzogen.

Eine optimale Bestellung erfolgt in vier Schritten:

- 1.** Unverbindliche und leichte Bestellvorbereitung – übersichtlicher Warenkorb mit allen Preisangaben und der Möglichkeit, jederzeit Waren daraus zu entfernen.
- 2.** Vorhandensein von personenbezogenen Eingabefeldern mit erkennbarer Trennung von Pflichtangaben und freiwilligen Informationen.
- 3.** Bewusste Bestellung, die dem Kunden durch eine zusätzliche Sicherheitsabfrage vor dem Kauf verdeutlicht wird und der er aktiv zustimmen muss.
- 4.** Empfangsbestätigung der Bestellung. Zu jeder Bestellung müssen Kundinnen und Kunden eine Empfangsbestätigung in angemessener Zeit erhalten, damit sie wissen, dass die Bestellung zugegangen ist. Sie soll ausdrückföhrig sein und per E-Mail zugesandt werden, sofern der Kunde eine E-Mail-Adresse angegeben hat.



Transparente Vertragsbedingungen

Das Internet ist weltumspannend. Die Anforderungen an die Vertragsbedingungen sind international in den unterschiedlichsten Rechtsordnungen geregelt. Deshalb legen die Gütesiegel ihr Schwergewicht auf Transparenz und Aufklärung. Vertragsbestimmungen und Allgemeine Geschäftsbedingungen (AGB) sollen eindeutig sein. Sie müssen bei Vertragsabschluss durch die Kundinnen und Kunden

- > abrufbar,
- > in wiedergabefähiger Form zu speichern sowie
- > ausdrucksfähig sein.

Zur Information über die Vertragsinhalte gehört auch die Kenntnis über das anwendbare Recht und den Gerichtsstand. Der Anbieter ist dafür verantwortlich, dass seine AGB dem jeweiligen nationalen Recht entsprechen und alle Informationspflichten erfüllen. Nennt der Anbieter einen Gerichtsstand, muss er ausdrücklich darauf hinweisen, dass der Verbraucher an dem Gericht, das für seinen Wohnsitz zuständig ist, auch klagen kann.

Sichere Bezahlung, Gewährleistung

Bezahlung im Internet muss nicht immer mit Datenrisiken verbunden sein. Gute Shops bieten:

- > Zahlungssysteme, die nicht allein dem Kunden das Risiko aufbürden (Vorsicht ist bei Versteigerungen oder Massenkäufen mit Vorausbezahlung geboten!),
- > kundenorientierte Zahlungsarten wie Lieferung gegen Rechnung oder Bezahlung per Lastschrift, bei der die Möglichkeit zum Rückruf besteht,
- > den Zeitpunkt des Bezahlvorgangs transparent an und rücken die Bezahlung möglichst in zeitliche Nähe der Lieferung.

Die Informationen zu den Zahlungsbedingungen müssen vollständig sein. Dazu gehören insbesondere:

- > umfassende Information über die Zahlungswege,
- > genaue Details über besondere Zahlungsbedingungen und -entgelte,
- > der Zeitpunkt des Zahlungsvorgangs bei Einzugsermächtigung, Kreditkartenzahlung oder einer elektronischen Bezahlweise,

- > Information über Datensicherheit bei elektronischen Bezahlvorgängen,
- > Wahrnehmung von Meldepflichten.

Lieferfristen, die eingehalten werden

Leistung und Lieferzeitpunkt gehören zu den wichtigsten Vorteilen beim Online-Shopping. Die gesetzlichen Fristen von 30 Tagen werden von den geprüften Shops in der Regel weit unterschritten. Wenn der geplante Liefertermin nicht eingehalten werden kann, verpflichten sie sich, die Kunden unverzüglich zu benachrichtigen. Dies ermöglicht den Kunden, vom Kauf zurückzutreten und ihre Ansprüche geltend machen zu können.

Garantie und Reklamation

Von höchster Bedeutung ist die Stelle, an die Garantieansprüche, Mängelrügen oder andere Beschwerden zu richten sind und von der sie auch bearbeitet werden. Kunden zertifizierter Shops dürfen nicht mit einem Anrufbeantworter abgespeist werden, der gelegentlich einmal abgehört wird. Der Anbieter muss telefonisch erreichbar

sein. Die Bearbeitung von Gewährleistungsansprüchen und die einfache Rückgabe der Ware müssen gesichert sein. Dies sind wichtige Rechte, wie sie etwa bei Käufen aus Versteigerungen über Online-Auktionsbörsen nicht bestehen.

Widerruf und Rückgabe

Die Möglichkeit, Widerrufsrechte auszuüben sowie die Angabe des Gerichtsstandes, an dem Ansprüche geltend gemacht werden können, sind unverzichtbar. Über folgende Rechte müssen Kundinnen und Kunden vor der Bestellung informiert werden:

- > mindestens 14 Tage Widerruf und Rückgaberecht (§ 312d BGB),
- > der Hinweis auf Ausnahmen muss vor Bestellung deutlich werden,
- > die Rückerstattung gezahlter Beträge muss innerhalb von 30 Tagen erfolgen,
- > die Rücksendekosten dürfen Kunden nur bei Bestellungen unter 40 Euro auferlegt werden,
- > der Wertersatz (Entschädigung) für den Gebrauch des Gegenstandes

darf nur bei vorherigem Hinweis (§ 357 Abs. 3 BGB) beansprucht werden.

Die Rückgabe soll für Kunden einfach per Formular möglich sein und Angaben enthalten, welche Kosten ggf. auf sie zukommen und wie die Rückerstattung bereits bezahlter Beträge erfolgt.

Eine besondere Leistung stellen »Geld-zurück-Garantien«, also Kaufpreisversicherungen dar, wie sie die beiden Gütesiegelanbieter Trusted Shops gemeinsam mit Gerling und TÜV Süd in Kooperation mit Winterthur Versicherungen gewähren. Damit wird den Kunden neben dem Beschwerdemanagement eine zusätzliche Sicherheit gewährt.

Datenschutz – dank Gütesiegel auf hohem Niveau

Datenschutz und Datensicherheit sind für Käufer entscheidende Fragen. Die Mehrzahl der Internetnutzer – nach Umfragen um 90 Prozent – kauft nicht bei Online-Shops, weil sie den Missbrauch ihrer Daten befürchtet.

Zum Schutz der personenbezogenen Daten sind zahlreiche nationale und internationale Vorschriften geschaffen worden:

- > Datenschutzgesetze des Bundes und der Länder (in Nordrhein-Westfalen ist die Landesbeauftragte für den Datenschutz auch für den privaten Datenschutz und damit für E-Commerce zuständig),
- > Teledienstegesetz,
- > Teledienstedatenschutzgesetz,
- > Telekommunikationsgesetz,
- > Telekommunikationsdatenschutzverordnung,
- > EU-Richtlinie 95/46 EG des EP und des Rates vom 24.10.1995,
- > EU-Richtlinie 97/66 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der Telekommunikation,
- > EU-Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr,
- > EU-Richtlinie 2002/58/EG. Datenschutzrichtlinie für elektronische Kommunikation.



Die Gütesiegel unterstützen Anbieter bei Umsetzung und Einhaltung der oben genannten Vorschriften.

Die Anbieter sollen auf der Hauptseite ihres Internetauftritts grundsätzlich eine Information zum Umgang mit personenbezogenen Daten und den Datenschutzprinzipien, die eingehalten werden, einstellen. Dies kann auch über einen internen Link geschehen.

Datensparsam wirtschaften

Informations- und Kommunikationsangebote sind unter dem Gütesiegel grundsätzlich schon bei der Einrichtung der Technik nach dem Prinzip der Datensparsamkeit zu gestalten. Dadurch werden so wenige Daten wie möglich erhoben, gespeichert und verarbeitet.

Dies ist nicht nur verbraucherfreundlich, sondern auch kostengünstig.

Die Erfassung von Kundendaten, die für die Erfüllung eines Vertrages unwesentlich sind, darf nicht in Abhängigkeit von Angebot und Leistung erfolgen. Umfangreiche Bedingungen dienen der Einhaltung der Gesetze

zum Schutz der Privatsphäre und der persönlichen Daten. Sie sind von allen geprüften Online-Shops zu erfüllen. Fragen nach Geschlecht, Alter (Ausnahme: Jugendschutz), Einkommen, Religion oder Staatsangehörigkeit der Kunden sind ebenso tabu wie die Klärung von Freizeitinteressen, Beruf, Familienstand oder Wohnverhältnissen.

Manche Firmen wollen solche Daten erfassen, um Kundenprofile zu erstellen und sie gegebenenfalls weiterzuverkaufen. Das ist zwar nicht verboten, aber das Gesetz schreibt vor, dass die Betroffenen darüber informiert werden müssen und ihre Einwilligung erforderlich ist.

Besonderer Jugenddatenschutz:

Angebote an Minderjährige dürfen nicht dazu benutzt werden, ohne Wissen und Einwilligung der Erziehungsberechtigten personenbezogene Daten (auch aus dem häuslichen Umfeld) zu erfassen, auszuwerten oder an Dritte weiterzugeben.

Weitere Rechte der Kunden

Die Kunden von Internet-Shops haben darüber hinaus das Recht, Auskunft über die zu ihrer Person gespeicherten Daten zu verlangen. Das gilt schon, bevor ein Geschäft abgeschlossen wird: Auch in der Angebotsphase liegt ein vertragsähnliches Vertrauensverhältnis vor.

Bei der Erhebung von Daten für Beratung, Werbung oder Marktforschung müssen die Kunden über den jeweiligen Zweck der Datenerhebung und das Widerspruchsrecht für die Zukunft aufgeklärt werden.

Grundsätzlich soll bei der Erhebung von Daten immer über deren Verwendungszweck informiert werden. Zu folgenden datenschutzrelevanten Sachverhalten sollten Aussagen getroffen werden:

- > Art und Umfang der verwendeten Daten,
- > Weitergabe personenbezogener Daten,
- > Behandlung der E-Mail-Adresse des Benutzers,
- > Einsatz von ActiveX, Java-Applets oder anderen aktiven Programmen,
- > Einsatz von Cookies,
- > Kontaktperson für datenschutzrelevante Fragen oder (sofern vorhanden) den betrieblichen Datenschutzbeauftragten,
- > Anspruch auf Auskunft und Berichtigung, Löschung oder Sperrung von Daten
- > Aufsichtsbehörde,
- > Einschaltung des Gütesiegelanbieters.

Sie können wählen

Anbieter von Telediensten sind gesetzlich verpflichtet, den Nutzern zwei Rechnungsvarianten anzubieten:

- > grundsätzlich eine Rechnung, die Zeitpunkt, Dauer, Art und Inhalt sowie Häufigkeit der Teledienste nicht erkennen lässt,
- > auf Verlangen der Nutzer einen Einzelnachweis, aus dem genau diese Details hervorgehen.

Die Homepage soll außerdem Hinweise zum Datenschutz und den zuständigen Aufsichtsbehörden enthalten.

Datensicherheit

Unsichtbare Angriffe gegen den Kunden-PC werden immer häufiger. Die Integrität und Authentizität der Anbieterinformationen müssen bei Nutzern durch ein geeignetes und dem Stand der Technik entsprechendes Sicherheitskonzept gewährleistet werden.

Zu schützen sind insbesondere die beim Anbieter betriebenen Verfahren und Einrichtungen, die Datenübertragungen zwischen Anbietern und Kunden betreffen. Sie sind zu verbessern,

zum Beispiel durch Einsatz einer Verschlüsselung wie SSL oder elektronischer Signatur. Bei der unbemerkten Datenübermittlung spielen »Cookies« eine wichtige Rolle. Dies sind kleine Dateien, die der Gegenseite im Datenverkehr angeboten und eingesetzt werden, um vom User oft unbemerkt Informationen über dessen Identität oder Online-Verhalten zu übermitteln. Gut, wenn die eingesetzten Cookies dem Kunden bekannt sind. Gesetzlich vorgeschrieben ist dies sogar, wenn dabei personenbezogene Daten verwendet werden. Cookies sollte man nur akzeptieren, wenn ihr Zweck und die Dauer ihrer Gültigkeit klar beschrieben werden. Darüber hinaus sind vielfältige illegale Angriffe über nicht systematisch gesicherte Homepages möglich, auch solche, von denen u.U. der betreffende Shop keine Kenntnis hat. Die Rede ist von so genannten »Dialern«. Dialer verändern illegal den Einwahlcode des PC ins Internet, leiten ihn über teure Telefonanschlüsse um und kassieren die Gebühren. »Trojaner« schleichen sich per E-Mail oder über andere Datentransfers auf die Festplatte des Computers und nehmen dort unbemerkt Manipulationen vor. Deshalb liegt es nicht nur im Interesse der Kunden und Kundinnen, sondern insbesondere im geschäftlichen Interesse jedes Internet-Shops, seine Systemkonfiguration und die der Geschäftskette, also aller Lieferanten und Kooperationspartner, entsprechend zu schützen.

Lösungen im Einvernehmen

Nach der Fernabsatzrichtlinie der EU und dem Fernabsatzgesetz der Bundesrepublik Deutschland sind die Rechte der Verbraucherinnen und Verbraucher bei Internet-Geschäften gestärkt worden. Dennoch ist der Rechtsweg vor allem in internationalen Online-Geschäften für die Regelung konkreter Beschwerden oft der umständlichere, langwierigere und nicht selten kostspieligere Weg, um Streitigkeiten zwischen Konsumenten und Unternehmen beizulegen.

Der Rechtsweg steht den Kunden immer am Gericht des eigenen Wohnorts offen: Die praktische Durchsetzbarkeit ist damit aber noch keineswegs garantiert. Die Kosten können schnell den Streitwert überschreiten, Sprachprobleme und Zuständigkeitskonflikte den Rechtsweg verstellen.

Alternative Streitschlichtung kann eine weitere wesentliche Voraussetzung sein, um das Vertrauen der Konsumentinnen und Konsumenten im elektronischen Geschäftsverkehr herzustellen.

Es sollten daher alternative Streitschlichtungsverfahren angeboten werden, die faire und kostengünstige Entscheidungen herbeiführen können, bevor der Rechtsweg beschritten werden muss. Dazu müssen unabhängige und glaubwürdige Schiedsverfahren für den globalen E-Commerce etabliert werden. Diese befinden sich noch im Aufbau.

Beschwerdemanagement

Gütesiegel verlangen: Der Anbieter muss eine Kontaktadresse angeben, an die der Kunde oder die Kundin sich bei Beschwerden per E-Mail, schrift-

lich und telefonisch wenden kann. Die Beschwerdeverfahren müssen angemessen und wirksam sein.

Die meisten Gütesiegel verpflichten sich, ein Beschwerdemanagement einzurichten, verfahren aber bisher nicht einheitlich. Beschwerden können über den Gütesiegelanbieter geregelt werden. Bei Trusted Shops erfüllt diese Aufgabe der Siegelanbieter selbst, ebenso das EuroHandelsinstitut. Bei VZ/OK wird die Verbraucherzentrale NRW tätig. S@fer-Shopping bietet bei Lieferproblemen die Unterstützung von Winterthur. Bei den meisten anderen Gütesiegeln können Beschwerden an deren Aufsichtsgremien gerichtet werden. Neben dem alternativen Streitschlichtungsverfahren wird ebenso eine von einer unabhängigen Instanz durchgeführte Mediation angestrebt.

Art und Umfang der Beschwerdeverfahren werden sich mit dem Ausbau des E-Commerce in den nächsten Jahren weiterentwickeln. Wichtig für Verbraucher ist, dass solche Möglichkeiten helfen können. Sie ersetzen aber nicht den Rechtsweg.





Bei Schiedsverfahren ist zu beachten, dass sie kostenfrei erfolgen und für den Kunden immer freiwillig sind. Wie Erfahrungen mit den Schlichtungsstellen der Handwerkskammern zeigen, funktionieren solche Modelle durchaus zur Zufriedenheit aller Beteiligten. Letztlich liegt es am guten Willen der Beteiligten und an der Zufriedenheit des Kunden, ob dieser nicht doch letztendlich den Weg zu Anwalt oder Gericht beschreitet. Nur wenn Verbraucherinnen und Verbraucher mit den vorgeschlagenen Lösungen zufrieden sind, sollten sie in die Ergebnisse einer solchen Schlichtung einwilligen.

Vertrauen ist gut – Kontrolle ist besser!

Die Echtheit von Gütesiegeln kann bei fast allen durch einen Klick auf das Symbol im Internet online überprüft werden.

Nutzer müssen wissen: Der Prüfaufwand ist je nach Größe des zertifizierten Unternehmens und der zu prüfenden Sicherheitsstufen unterschiedlich hoch. Nicht jedes Siegel setzt den

gleichen Kontrollaufwand voraus. Das Einpersonen-Unternehmen, das 25 Artikel anbietet, hat einen geringeren Aufwand, bestimmte Sicherheits- und Gewährleistungsanforderungen zu erfüllen als die Online-Buchungsabteilung eines großen Reiseunternehmens mit mehreren hundert Mitarbeiterinnen und Mitarbeitern. Für die Kundschaft sollen sich aber die Sicherheitsstandards am Ende möglichst nicht unterscheiden. Bestimmte Mindestanforderungen werden erfüllt und unterschiedliche Wege beschritten, um etwa auch bei kleineren Firmenbudgets den Erwerb eines Siegels zu ermöglichen. Kostengünstiger muss dabei nicht immer schlechter heißen, denn es kommt darauf an, an welcher Stelle beispielsweise aufwändige Prüfläufe vereinfacht werden oder auf Kontrollen vor Ort zunächst verzichtet wird. Entscheidend für die unterschiedlichen Konzepte sind bisher neben Risikoanalysen die Erfahrung und Philosophie des jeweiligen Gütesiegel-Unternehmens. Klar ist, dass die beste Selbstauskunft eine Prüfung vor Ort nicht ersetzen

kann. Siegel, die auf eine Prüfung vor Ort verzichten, können »schwarze Schafe« vielleicht nicht im Vorhinein erkennen. Sie setzen deshalb in besonderem Maße auf das Feedback der Kunden. Nicht unwesentlich sind auch die Konsequenzen, die dem Unternehmen bei Verletzung der Pflichten, die mit den Gütesiegeln verbunden sind, drohen. Schon vor dem Entzug des Siegels sind strenge Fristen, Vertragsstrafen und natürlich die Drohung mit der Veröffentlichung des Siegelentzuges wirkungsvolle und notwendige Sanktionen, um Mängel abzustellen.

| Was leisten Gütesiegel?

Einige Beispiele, was Siegel leisten und worin sie sich voneinander unterscheiden:

> **Qweb – DIN CERTCO**

Das Gütesiegel von DIN CERTCO wird derzeit überarbeitet. Bei Drucklegung der Broschüre lag noch keine Konformitätserklärung des neuen Siegels vor.

> **Geprüfter Online Shop – EuroHandelsinstitut**

Gültigkeit 1 Jahr. Folgeprüfung jährlich, Kontrollprüfung bei Beschwerden. Zertifizierung der Datenschutzstandards durch T-Systems – T-Systems ISS GmbH, Bonn. Überprüfung von Qualitätsstandards und Leistungen anhand Checkliste durch eigene Betriebswirte und Wirtschaftsinformatiker. Testkäufe. Prüfkriterien und -verfahren entsprechen www.euro-label.com. Kostenfreies Beschwerdemanagement. Siegelvergabe durch den Fachbeirat. Sanktionen: Entzug des Siegels.

> **TÜV Online Check-VZ OK – RWTÜV mit der Verbraucherzentrale NW**

Gültigkeit 1 Jahr, Zwischenprüfung nach 6 Monaten vor Ort. Kontrolle bei Beschwerden. Mitarbeiter des TÜV und der Verbraucherzentrale, Qualitätsmanager und IT-Spezialisten. Umfangreiche Kontrollen vor Ort sowie Online-Checks und Testkäufe. Prüfung: 50 % vor Ort, 25 % online, 25 % Testkäufe. Sanktionen: Siegelentzug, Veröffentlichung durch Verbraucherzentrale.

> **Trusted Shops – Trusted Shops GmbH mit Gerling Konzern**

Gültigkeit 1 Jahr, Folgeprüfung jährlich. Fortlaufende Prüfungen der bestimmungsgemäßen Verwendung des Siegels. Finanzielle, technische und organisatorische Überprüfung durch IT-Personal von TS und Wirtschaftsprüfer (Gerling Konzern). Bonitätsprüfung,

u. a. Sichtung der Bilanzen. Mitarbeiter von Trusted Shops, durch die Impact-Unternehmensberatung geschult. Zertifizierung durch schriftliche Prüfung und online, bei größeren Händlern Besuche vor Ort. Testkäufe. Kontrollen bei Beschwerden. Sanktionen: gestaffeltes System bei Beschwerden und Nichteinhaltung von Bestimmungen oder Meldepflichten. Fristsetzung zur Abstellung von Mängeln max. 10 Tage, dann Vertragsstrafen bis zu 15.000,- Euro oder Entzug des Siegels. Meldung an Verbraucherschutzorganisationen, Veröffentlichung.

> **WebTrust Programm – IDW Net GmbH**

Gültigkeit 1 Jahr, innerhalb dieses Zeitraums sind regelmäßig aktualisierende Prüfungshandlungen vorzunehmen. Prüfung durch lizenzierte Wirtschaftsprüfer, die über besondere Kenntnisse für die Durchführung der WebTrust-Prüfungen verfügen. Vor Ort Prüfung von Geschäftspraktiken, Geschäftsabwicklung, Datenschutz und Datensicherheit sowie des Kontrollsystems. Transaktionstests und Tests der Sicherheitsmaßnahmen. Sanktionen: Entzug des Siegels.

> **TÜVIT – TÜV Informationstechnik GmbH**

Gültigkeit: nicht begrenzt, Datum der Erteilung ist Bestandteil des Siegels. Zertifizierungsstelle prüft die Verwendung des Siegels. Prüfung durch hoch qualifiziertes IT-Personal, Prüfberichte werden von Zertifizierungsstelle überprüft. Sicherheitsprüfungen vor Ort, fingierte System- und Hackerangriffe. Sanktionen: Fristen zur Abstellung von Mängeln, Entzug des Siegels.

> **Certified e-Business – PECOS AG**

Gültigkeit: 1 Jahr, Kontrolle alle 4 Monate, Reaudit nach 1 Jahr. Prüfung durch Mitarbeiter der PECOS AG, durch akkreditierte Zertifizierer wie Wirtschaftsinformatiker, DV-Spezialisten und Qualitätsmanager (QM). Prüfungsanteile 50 % vor Ort, 50 % online, Testkäufe und aufwendige fingierte Datensystemangriffe. Sanktionen: Entzug des Siegels.

> **TÜV Secure IT – TÜV Rheinland/Berlin/Brandenburg**

Gültigkeit: 1 Jahr, jährliches Monitoring durch TÜV Secure IT Audit. Erneuerung nach 1 Jahr. Prüfung durch Mitarbeiter, IT- und QM-Fachleute, Ingenieure 50 % vor Ort, 50 % online. Testkäufe und umfangreiche Checks des Datensystems finden statt. Sanktionen: Entzug des Siegels bei Abweichungen oder Verstößen.

> **S@fer Shopping – TÜV Management Service, Unternehmensgruppe TÜV Süddeutschland**

Gültigkeit: unbegrenzt, jährliche Überprüfung, jederzeit besteht die Möglichkeit unangemeldeter Online-Checks. Technische und organisatorische Prüfung durch eigene IT-Spezialisten, Security-Fachleute, Spezialisten für Softwareergonomie und Qualitätsmanagement. Bonitätsprüfung durch Winterthur-Garantie, DBV-Winterthur-Versicherung. Etwa 40 % vor Ort, 40 % online, 20 % Dokumente und Berichte. Fingierte Testkäufe, bei denen Benutzerfreundlichkeit und Kundenzufriedenheit über längeren Zeitraum getestet werden. Sanktionen: Entzug des Siegels.

| Warum die Gütesiegel der Initiative D21?

Das Problem mangelnden Vertrauens in Internetgeschäfte ist bekannt. Nicht nur seriöse Anbieter versuchen deshalb, mit Gütesiegeln oder Zertifikaten das

Vertrauen potentieller Kunden zu wecken. Die Initiative D21 hat sich auf ein hohes gemeinsames Niveau ihrer Anforderungen geeinigt. Die Mitglieds-

unternehmen arbeiten nach dem Prinzip der Selbstkontrolle zusammen und entwickeln Prüfkriterien und Mindeststandards ständig weiter.

<p>Markteinführung eines neuen Gütesiegels in Vorbereitung</p> <p>DIN CERTCO Gesellschaft für Konformitätsbewertung mbH Postfach 301107 D-10772 Berlin Tel.: +49 (0) 30 - 26 01-2108 Fax: +49 (0) 30 - 26 01-1610 zentrale@dincertco.de www.dincertco.de</p>	 <p>EHI-EuroHandelsinstitut Spichernstr. 55 D-50672 Köln Tel.: +49 (0) 2 21 - 5 79 93-63 Fax: +49 (0) 2 21 - 5 79 93-46 info@shopinfo.net www.shopinfo.net</p>	 <p>Verbraucherzentrale NW e. V./ RWTÜV Anlagentechnik GmbH Fachbereich Zertifizierung Kurfürstenstraße 58 D-45138 Essen Tel.: +49 (0) 2 01 - 8 25-3269 Fax: +49 (0) 2 01 - 8 25-3307 Kesting@rwtuev-at.de www.tuev-online-check.de</p>
 <p>Trusted Shops GmbH Im Mediapark 8/KölnTurm D-50670 Köln Tel.: +49 (0) 2 21 - 7 75 36-6 Fax: +49 (0) 2 21 - 7 75 36-89 info@trustedshops.de www.trustedshops.de</p>	 <p>IDW Net GmbH Institut der Wirtschaftsprüfer in Deutschland e. V. Tersteegenstraße 14 D-40474 Düsseldorf Tel.: +49 (0) 2 11 - 45 61-0 Fax: +49 (0) 2 11 - 45 61-233 Info@idwnet.de www.idw-verlag.com</p>	 <p>TÜV Informationstechnik GmbH Am Technologiepark 1 Gebäude A6 D-45307 Essen Tel.: +49 (0) 2 01 - 89 99-420 Fax: +49 (0) 2 01 - 89 99-444 Info@tuvit.de www.trusted-site.de</p>
 <p>PECOS AG Musilweg 2 D-21079 Hamburg Tel.: +49 (0) 40 - 23 78 13-0 Fax: +49 (0) 40 - 23 78 13-240 info@pecos.de www.pecos.de</p>	 <p>TÜV Secure IT GmbH Unternehmensgruppe TÜV Rheinland/Berlin/Brandenburg Am Grauen Stein D-51101 Köln Tel.: +49 (0) 2 21 - 8 06-2560 Fax: +49 (0) 2 21 - 8 06-1580 secureit@de.tuv.com www.tuv.com</p>	 <p>TÜV Management Service GmbH Unternehmensgruppe TÜV Süddeutschland, Ridlerstraße 65 D-80339 München Tel.: +49 (0) 89 - 57 91-4297 Fax: +49 (0) 89 - 57 91-2544 info@safer-shopping.de www.tuev-sued.de</p>

| Selbst sicherer im Internet

Ausgangspunkt jeder Kommunikation und jedes Geschäfts im Internet ist der PC. Viele Risiken, die in dieser Broschüre beschrieben werden, aber auch solche, auf die hier nicht eingegangen werden kann, können mit einfachen Mitteln erkannt und verringert werden. Außer einem Anti-Virenprogramm sind hierfür keineswegs immer aufwendige Soft- und Hardwareinstallationen notwendig.

Nähere Informationen, wie man mehr für den Schutz eigener Daten tun kann, geben die Datenschutzbeauftragten von Bund und Ländern. Sie sind erreichbar über die gemeinsame Homepage www.datenschutz.de.

Außerdem sind darüber auch die Datenschutzbeauftragten von Körperschaften und Religionsgemeinschaften und internationale Datenschutzstellen erreichbar.

Einen interessanten Dienst für alle PC bieten der niedersächsische und der Datenschutzbeauftragte des Kantons Zürich in Verbindung mit der Hochschule für Technik Rapperswil kostenlos an:

Per »Browser-Diagnose« können User erfahren, welche Daten der Computer preisgibt und wie die Gefahrenstufe des PC-Systems einzuschätzen ist. Das System gibt auch leicht verständliche Hinweise, wie durch die Deaktivierung von Anwendungen sofort mehr Vertraulichkeit geschaffen werden kann.

Adressen:

www.lfd.niedersachsen.de/service/service_selbstt.html oder www.datenschutz.ch

Außerdem bieten die Datenschutzbeauftragten kostenlose Programme zur Erhöhung der Sicherheit an. So etwa JAP Java Anon Proxy zum Surfen im Internet ohne Preisgabe der eigenen Identität oder PGP (Pretty Good Privacy), ein Verschlüsselungs- und Entschlüsselungssystem für E-Mails.

Warum nutzen Gütesiegel dem E-Business?

Datensicherheit ist ein entscheidender Vorteil für jedes Unternehmen. Für Kunden und Verbraucher sind hohe Standards, die durch ein Gütesiegel unterstrichen werden, das entscheidende Argument für diese neue Einkaufsart. Das zahlt sich vor allem für neue Shops und Start-ups aus, denn sie verfügen noch nicht über den Namen, mit dem die Käufer bei etablierten Unternehmen bereits ein bestimmtes Grundvertrauen verbinden. Aber die Datenschutz- und Datensicherheitsprüfungen der Gütesiegel leisten mehr, denn sie:

- > verbessern die Standards der Informationstechnik dauerhaft,
- > sorgen für ein höheres Sicherheitsniveau und eine Risikominderung gegenüber Hackerattacken und Virenangriffen,
- > verbessern die Prozessabläufe und sichern die Informationskette zwischen Shop, Lieferanten, Lagern und Versandlogistik, Dienstleistern und Kunden,
- > bringen Rechtssicherheit und Versicherbarkeit gegen Angriffe auf das System,
- > schaffen durch Backups und übergeordnete Systemkontrollen auch

Sicherheit gegen Angriffe des eigenen Personals oder der Fernwartung, > schaffen Vertrauen bei Geschäftspartnern und Kunden.

Virenattacken, Hacker oder andere Angriffe missgünstiger oder geschäftsschädigender Zeitgenossen werden immer raffinierter. Im Zertifizierungsprozess werden die Anbieter dazu angeleitet, ihre Systeme durch geeignete »Firewalls« zu schützen.

Finanzielle Risiken mindern

Gerade für kleinere Internetunternehmen ist die Eigensicherung des Systems von großer Bedeutung. Systemausfälle können unkalkulierbare wirtschaftliche Risiken bergen. Überlastungsattacken wie DDOS (engl.: = Distributed Denial of Service) können Systeme in kurzer Zeit lahm legen. So bedeutet eine Stunde Systemausfall für Großanbieter wie Amazon.com einen Verlust von 244.000 US-Dollar, für die Kreditkartenbranche liegt ein solcher Schaden bei etwa 3,1 Millionen US-Dollar pro Stunde!

Angriffe auf die IT-Sicherheit müssen aber nicht immer von außen kommen. Gerade für mittlere und größere Unternehmen spielen auch Sicherungen gegen interne Datensabotage eine immer wichtigere Rolle. So richtete ein gekündigter Mitarbeiter bei »Omega Services« mit einem 6 Zeilen langen Computerbefehl in Sekundenschnelle 10 Millionen US-Dollar irreparablen Schaden an.

Sicherer E-Commerce lohnt sich für alle!

Sicherer E-Commerce ist wirtschaftlich. Er lohnt sich für Verbraucher und für die Unternehmen in jedem Fall.

Für Unternehmen bedeutet die Zertifizierung:

- > sichere Bestellungen, eine geringere Rate an Kaufabbrüchen und damit Steigerungschancen für den Umsatz,
- > höhere Kundenzufriedenheit durch benutzerfreundlichere Shopangebote und leichtere Auffindbarkeit der Produkte,
- > mehr Sicherheit bei Datenangriffen und Systemausfall,
- > Überprüfung und Optimierung der Prozesse und der eigenen Leistungsfähigkeit,
- > Dokumentation der Geschäftsabläufe und ihrer Sicherheit und Vertrauenswürdigkeit durch unabhängige Dritte.



**Das gemeinsame Ziel:
Mehr Vertrauen bei Kunden
und Lieferanten!**

| Stichwörter und Abkürzungen

After sales	Betreuung und Kontaktpflege, Information und Beschwerdemanagement nach dem Kauf.
AGB	Allgemeine Geschäftsbedingungen. Sie sollten vor einem Kauf immer gelesen werden. Das AGB-Gesetz schützt die Verbraucher vor risikoreichen oder unseriösen Geschäftspraktiken. Die AGB sollten im E-Commerce leicht anklickbar sein.
B2B	Business to Business. Geschäftsbeziehung zwischen gewerblichen Vertragspartnern.
B2C	Business to Consumer. Geschäftsbeziehung zwischen gewerblichen Anbietern und privaten Kunden.
BS 7799	BS: British Standard ISO/IEC 17799 (BS 7799-1) ist ein internationaler Leitfaden für das Management der Informationssicherheit. Der zertifizierbare Teil BS 7799-2:2002 ist eine Spezifikation für einzelne Anforderungen zur Definition, Implementierung und Dokumentation eines Informationssicherheits-Management-systems. Er bietet eine Grundlage für die Bewertung des Systems.
Cookies	Kleine Dateien, die von der »Gegenseite« auf der Computerfestplatte des Angegriffenen platziert werden und vereinfachte Identifikation ermöglichen, aber auch illegale Informationen und Verhaltensprofile übermitteln können.
Cybercoin	Elektronische Bezahlform mit 1024 Bit – Verschlüsselung. Ähnlich: E-Cash.
DDOS	Distributed Denial of Service. Gezielte Überlastung eines elektronischen Systems durch eine Vervielfachung von Kundenanfragen oder E-Mails. Wurde im Frühjahr 2000 gegenüber internationalen Konzernen eingesetzt. Ähnlich der 2001 angemeldeten »elektronischen Demonstration« gegen die Durchführung von Abschiebungen durch die Deutsche Lufthansa.
Dialer	Illegale, per Datenangriff von außen heimlich veränderte Einstellung der Einwahlmechanismen eines PC oder Computersystems ins Netz, durch die die Zielobjekte des Angriffs abkassiert werden.
Initiative D21	Zusammenschluss moderner, innovativer Unternehmen in Deutschland auf Initiative von Bundeskanzler Schröder zur Förderung neuer Techniken, des E-Commerce und der IuK-Techniken. Im »Board« Selbstregulierung sind die in dieser Broschüre vorgestellten Siegelanbieter organisiert.
Elektronische Signatur	Rechtsverbindliche, eindeutig identifizierbare, vertrauliche und verbindliche Unterschrift und Willenserklärung im elektronischen Verkehr. Identität und Zertifizierung durch Trust-Center.
E-Business	Elektronisch abgewickelte Geschäfte, nicht nur im Internet.
E-cash	Elektronische Bezahlform, die u. a. von einer deutschen Großbank erprobt wurde. Spezielle Software erforderlich.
Ecin	www.ecin.de: Informationssystem Electronic Commerce Info Net ist eine aktuelle Informationsquelle für E-Commerce im Internet mit Expertenartikeln und Veranstaltungshinweisen.
E-Commerce	Elektronischer Handel. Gemeint sind alle elektronisch vermittelten Geschäftsprozesse.
E-Commerce Center Handel	www.ecc-handel.de: Vom Bundeswirtschaftsminister geförderte Initiative unter der Leitung des Instituts für Handelsforschung an der Uni Köln. Bietet branchenspezifische Informationen zum elektronischen Handel.
Fernabsatzgesetz	Konkretisiert die Fernabsatzrichtlinie der EU. Zum Teil wesentlich konkretere und datenschutzfreundlichere Vorschriften sowie Bestimmungen über die elektronische Signatur.

Fernabsatzrichtlinie	Am 1.1.2001 in Kraft getretene Richtlinie der EU, die neben den Bestimmungen über elektronische Signatur auch Mindeststandards für E-Commerce festlegt. So wird z. B. allen Konsumenten das Recht zur Klageerhebung gegen weltweite Geschäftspartner in ihrem Heimatstaat garantiert.
Firewall	Elektronische Sicherheitsinstallation, die Computer und Computersysteme gegen Viren- und Hackerangriffe schützt.
Geldkarte	EC-Scheckkarte, die mit POS den in Deutschland weit verbreiteten Lastschrifteneinzug ablösen soll.
Infoletter »e-facts«	Informationen zum E-Commerce. Informationsschrift zum Thema, erhältlich beim Bundeswirtschaftsminister unter www.bmwi.de/unternehmen/e-business .
Initiative Media Mit	www.mediamit.de : Initiative des Deutschen Industrie- und Handelskammertages DIHK für kleinere und mittlere Unternehmen zu E-Commerce.
Integrierte Software	Softwareoberflächen für den elektronischen Handel, die durchgängig mit den gleichen Datensätzen arbeiten.
IK-Technik	Informations- und Kommunikationstechnik
ISO 9001 DIN EN ISO 9000	Standard für Qualitätsmanagement und die Optimierung von Unternehmensabläufen. ISO 9001 (DIN EN ISO 9000) gibt die Forderungen an Qualitätsmanagementsysteme für den Fall an, dass eine Organisation ihre Fähigkeit demonstrieren muss, Produkte oder Dienstleistungen bereitzustellen, so dass sie den Erfordernissen des Kunden und den gesetzlichen und behördlichen Anforderungen entsprechen.
JAP	Java Anon Proxy. Software zum unerkannten Surfen im Internet.
Konformität	Hier: Übereinstimmung durch Erklärung der im Board D21 kooperierenden Anbieter von Gütesiegeln zur Einhaltung von vereinbarten Mindeststandards.
LfD	Landesbeauftragte für den Datenschutz in NRW: www.lfd.nrw.de .
Millicent	Elektronische Münzen, die für Kleinbeträge eingesetzt werden. Geringe Datensicherheit. Angeboten von DEC (Digital Equipment).
Netcash	Mit PGP verschlüsseltes elektronisches Münzbezahlsystem. Die Schwachstelle ist die zentrale Speicherung der Seriennummer, über die feststellbar ist, wer was wann und wo gekauft hat.
Net Cheque	Elektronischer Scheckverkehr, entwickelt von der University of South Carolina. Anlehnung an Schecks, nicht anonym, ähnlich elektronischer Überweisung.
Netzwerk elektronischer Geschäftsverkehr	www.bmwi-netzwerk-ec.de . Detaillierte, auf kleine und mittlere Unternehmen zugeschnittene Informationen und Veranstaltungstipps.
Online-Shopping	= Internet Shopping. Geschäftsvorgänge über das Internet.
PGP	»Pretty good Privacy«. U. a. von den Datenschutzbeauftragten von Bund und Ländern und vom »Chaos Computer Club« empfohlener Verschlüsselungsstandard.
Paybox, Payitmobile, Streetcash	Bezahlsysteme über das Handy. Registrierung beim Anbieter, Bezahlung über PIN und Bestätigung per SMS. Kritik von Verbraucherschützern wegen Gefahr der Einsehbarkeit der PIN-Eingabe.

POS	Point of Sales. Datengestütztes Bezahlsystem, wie z. B. in Deutschland die von mehreren Banken eingeführte Geldkarte, mit der per elektronischer Abbuchung eines Geldbetrages vom Mikrochip direkt im Geschäft elektronisch bezahlt wird. Bis jetzt hat sich POS, auch wegen Datenschutzproblemen (Konsumentenprofile), nicht gegen die verbraucherfreundlichere und datensichere Lastschriftzahlung per EC-Karte durchsetzen können.
Privacy Statement	Datenschutzbestimmungen einer Homepage oder eines Anbieters, die – ähnlich wie die AGB – von allen Seiten eines Internetshops leicht erreichbar sein sollten.
Privacy Policy Statement Generator	Für die Gestaltung einer Privacy Policy für den E-Commerce hat die OECD ein Tool bereitgestellt: Privacy Policy Statement Generator. http://cs3hq.oecd.org/scripts/pwv3/pwhome.htm .
Qualitätsmanagement (QM)	Aufeinander abgestimmte Tätigkeiten zur Leitung und Lenkung einer Organisation bezüglich der Qualität. Leitung und Lenkung von Qualität umfassen üblicherweise die Festlegung der Qualitätspolitik, Formulierung von Qualitätszielen, die Qualitätsplanung, Qualitätslenkung, Qualitätssicherung und Qualitätsverbesserung.
SET = Secure Electronic Transaction	Verdecktes Bezahlsystem, bei dem der Händler eine Bezahlgarantie, aber keine Daten bekommt. Der Verbraucher genießt Datensicherheit und die Bank erfährt nichts über den gekauften Gegenstand. Visa, Mastercard und viele andere Partner. Softwareinstallation und Bankakkreditierung erforderlich.
SSL = Secure Socket Layer	SSL ist eine Verschlüsselungstechnik für Kreditkartenbezahlung, die u. a. von Netscape und Nachfolgern angeboten wird. US-Verschlüsselung mit 128-Bit sicher, internationale 40-Bit nicht.
Tagespreise	Besondere Angebote von E-Commerce-Unternehmen, deren Zeitdauer begrenzt ist. Deshalb kommt es bei der Systemkonfiguration des Shops darauf an, dass verlässliche und ausdrucksfähige Bestätigungen über den Bestellzeitpunkt vorgesehen und Manipulationsmöglichkeiten ausgeschlossen werden.
Teledienste	Pro Zeiteinheit abgerechnete Online-Dienste. Für diese sind zwei Arten von Abrechnungen vorgesehen: eine anonymisierte Gesamtrechnung aller Leistungen ohne Identifizierbarkeit der einzelnen Vorgänge oder einen offenen Einzelnachweis aller genutzten Leistungen mit Datum und Zeitdauer.
Trojaner	Spezielles Virus, das sich an E-Mails oder andere elektronische Inhalte unbemerkt anhängt und das System des Zielcomputers manipuliert, Informationen z. B. kopiert und an den Absender zurücksendet.
Viren	Gefährliche elektronische Mikroorganismen, die Dateninhalte zerstören, verfremden und verfälschen können.
Warenkorb	Hilfsmittel bei der Durchführung eines Internet-Bestellvorgangs, um die einzelnen Waren und Preise sowie die Gesamtsumme und alle Nebenkosten erkennbar zu machen, ohne dass bereits ein Kaufvertrag zustande gekommen ist.
Wurm	Abart eines Virus, das sich zumeist an E-Mails anhängt und sich selbstständig durch unbemerkte Produktion weiterverbreitet und die gesamte Oberfläche für elektronischen Briefverkehr verseuchen kann.
Zweckbindungsgebot	Verfassungsrechtliches Gebot aus dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983. Danach dürfen Daten nur soweit erhoben, verarbeitet und gespeichert oder weitergegeben werden, als sie zur Erreichung des Zwecks unbedingt erforderlich sind.



| Adressen und Informationen zum E-Commerce

www.lfd.nrw.de	Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen ist zuständig für Datenschutzbeschwerden gegen die öffentliche Verwaltung und die private Wirtschaft. Reichsstraße 43 40217 Düsseldorf Tel.: +49 (0) 2 11 - 3 84 24-0 Fax: +49 (0) 2 11 - 3 84 24-10 E-Mail: datenschutz@lfd.nrw.de
www.shopfinder.de www.markt-treff.com www.shoppingservice.com www.shops.de	Shopping-Guide für das Internet Allgemeine Informationen zum E-Commerce
www.shopsuche.de	Suchmaschinen für die Suche nach Internet-Shops
www.vz-nrw.de	Verbraucherzentrale Nordrhein-Westfalen e.V. Mintropstraße 27 40215 Düsseldorf Tel.: +49 (0) 2 11 - 38 09-0 Fax: +49 (0) 2 11 - 38 09-172 E-Mail: vz.nrw@vz-nrw.de
www.mwa.nrw.de	Ministerium für Wirtschaft und Arbeit des Landes Nordrhein-Westfalen Referat Presse und Öffentlichkeitsarbeit 40190 Düsseldorf Fax: +49 (0) 2 11 - 8 37-2200 www.mwa.nrw.de

| Kontakt

Agentur »secure-it.nrw.2005«
bei der IHK Bonn/Rhein-Sieg
Bonner Talweg 17
53113 Bonn
Tel. +49 (0) 2 28 · 22 84-184/185
Fax +49 (0) 2 28 · 22 84-221
info@secure-it.nrw.de
www.secure-it.nrw.de

Ministerium für
Wirtschaft und Arbeit
des Landes
Nordrhein-Westfalen
Referat Presse und Öffentlichkeitsarbeit
40190 Düsseldorf
Fax +49 (0) 2 11 · 8 37-22 00
www.mwa.nrw.de

2003 / MWA 1367

Diese Druckschrift wird im Rahmen der Öffentlichkeitsarbeit der Landesregierung Nordrhein-Westfalen herausgegeben. Sie darf weder von Parteien noch von Wahlwerbern oder Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für Landtags-, Bundestags- und Kommunalwahlen sowie für die Wahl des Europäischen Parlaments. Missbräuchlich ist besonders die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen und Werbemittel. Untersagt ist gleichfalls die Weitergabe an Dritte zum Zwecke der Wahlwerbung. Eine Verwendung dieser Druckschrift durch Parteien oder sie unterstützende Organisationen ausschließlich zur Unterrichtung ihrer eigenen Mitglieder bleibt hiervon unberührt. Unabhängig davon, wann, auf welchem Weg und in welcher Anzahl diese Schrift dem Empfänger zugegangen ist, darf sie auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl nicht in einer Weise verwendet werden, die als Parteinahme der Landesregierung zugunsten einzelner politischer Gruppen verstanden werden könnte.



www.secure-it.nrw.de
www.mwa.nrw.de



Ministerium für
Wirtschaft und Arbeit
des Landes
Nordrhein-Westfalen

NRW.

SECURE IT