



# Datenschutz in der Informationsgesellschaft

*Dr. Severin Löffler,*

*Leiter Recht & Politik, Mitglied der Geschäftsleitung Microsoft Deutschland GmbH*

## 1 | Verlässlicher Umgang mit Daten hat Priorität

Je mehr Menschen Computer und Internet nutzen, desto mehr Informationen werden übertragen. Dabei wollen die Nutzer darauf vertrauen können, dass ihre persönlichen Daten in guten Händen sind. Gleichzeitig wollen sie genau wissen, was mit ihren Daten geschieht. Als Anbieter von Technologien und Services hat Microsoft sich deshalb zum Ziel gesetzt, verlässliche Lösungen zu schaffen und für die nötige Transparenz zu sorgen. Denn Vertrauen ist eine der wichtigsten Voraussetzungen für die Akzeptanz und Nutzung von Informationstechnologien. Nur Anwender, die sich uneingeschränkt sicher fühlen, schöpfen die Möglichkeiten des Internets aus. Beispielsweise möchten sie, wenn sie die Vorteile individueller Dienste nutzen, die Kontrolle über ihre persönlichen Daten behalten. Vor allem bei Anwendungen wie Suchmaschinen, personalisierten Online-Services und Online-Werbung ist Datenschutz wichtig.

Für Unternehmen hat der sorgfältige Umgang mit Kundendaten ebenfalls große Bedeutung und stellt ein Qualitätsmerkmal dar, von dem auch der Geschäftserfolg abhängen kann. Allein der Verdacht auf mögliche Unsicherheiten im Umgang mit sensiblen Daten kann die Wettbewerbsfähigkeit eines Unternehmens ernsthaft gefährden und dessen Ruf beschädigen. Zudem müssen Unternehmen sicherstellen, dass sie gesetzliche Richtlinien einhalten (Compliance). Unter anderem gilt es, bestimmte Informationspflichten zu erfüllen, wobei der sichere Umgang mit Daten eine wichtige Rolle spielt.

### 1.1 | Datenschutz gewinnt an Brisanz

Das Verständnis von Sicherheit hat sich in den vergangenen Jahren stark verändert. Es geht nicht mehr nur um den Schutz von Computern und der Netz-

### Dr. Severin Löffler

*ist seit Oktober 2008 als Senior Director Legal and Corporate Affairs bei der Microsoft Deutschland GmbH tätig. In dieser Funktion leitet er die Bereiche Legal und Corporate Affairs. Severin Löffler berichtet an Dorothee Belz, Associate General Counsel EMEA, und ist Mitglied der Geschäftsleitung der Microsoft Deutschland GmbH.*

*Er startete seine Laufbahn als Rechtsanwalt bei der Kanzlei Friederich, Ernst, Engelhard & Partner in München. Vor seinem Start bei Microsoft arbeitete er sieben Jahre bei der internationalen Großkanzlei Clifford Chance. Der Volljurist promovierte im internationalen Medienrecht.*



Infrastruktur vor Hackern und Schadprogrammen. Sondern auch darum, den Zugriff auf gespeicherte Daten zu kontrollieren. Das betrifft Informationen für Online-Banking auf dem Privat-PC genauso wie vertrauliche Kunden- und Finanzdaten auf Servern von Unternehmen und Behörden.

Außerdem hat Datenschutz für die Anwender eine größere Bedeutung bekommen. Das ergab die Microsoft-Sonderbefragung „Sicher Surfen 2008: Wie schützen sich Onliner im Internet?“ im Rahmen des (N)Onliner Atlas 2008 von der Initiative D21 und TNS Infratest. Im Mittelpunkt des Interesses der Befragten stehen nicht mehr wie in den Jahren zuvor Viren und Trojaner. Vielmehr gewinnt das Thema Datenschutz an Brisanz. 22 Prozent der Befragten möchten mehr über die Sicherheit ihrer Daten erfahren – das sind 15 Prozentpunkte mehr im Vergleich zum Vorjahr und damit ein Anstieg um das Dreifache.

### 1.2 | Welche Daten geschützt werden müssen

Daten entstehen bei fast allen Anwendungen – beim Einkaufen und Surfen im Internet oder bei der Text-

erstellung mit Office-Programmen. Überall hinterlässt der Nutzer seine Spuren. Zum Teil direkt, beispielsweise wenn er im Internet Formulare ausfüllt; zum Teil auch indirekt durch Metadaten in Dokumenten, der IP-Adresse oder Cookies.

Informationen, die Rückschlüsse auf den Nutzer zulassen, bedürfen eines besonderen Schutzes. Dies sind zum einen pseudonyme Daten, die zwar den Nutzer nicht eindeutig identifizieren, aber mit ihm assoziiert werden könnten. Beispielsweise Informationen und Profile von Nutzern, die nicht an ein Individuum gebunden sind. Zum anderen gibt es persönliche Informationen. Sie lassen sich einer Person genau zuordnen, dazu gehören Name, E-Mail-Adresse, Kreditkartennummer und biometrische Daten. Einige dieser Angaben, wie Passwörter oder PIN, sind so sensibel, dass sie speziell geschützt werden müssen.

## 2 | Datenschutz in der Praxis

### 2.1 | Unternehmen: Datenschutz schafft Vorteile

Unternehmen erheben Kundendaten aus unterschiedlichen Gründen. Beispielsweise können sie damit einen persönlicheren Service bieten. Kennen sie Verhalten und Vorlieben ihrer Kunden, können sie außerdem innovative Geschäftsfelder entwickeln. Wenn sie sorgfältig mit diesen Informationen umgehen, verschafft ihnen das einen Wettbewerbsvorteil. Damit die Daten von Kunden und auch Mitarbeitern gut geschützt sind, sollten Unternehmen über den gesamten Lebenszyklus einer Information für deren Sicherheit sorgen (Data Governance Lifecycle). Das beginnt schon beim Erheben und Sammeln der Daten. Beispielsweise sollten Kunden die Wahl und Kontrolle haben, welche Informationen sie preisgeben möchten. Bei der Speicherung und Nutzung gelten ebenfalls Sicherheitsanforderungen. Unter anderem muss das Unternehmen den Zugang regeln und die Daten vor Missbrauch schützen. Schließlich sollte die sichere Archivierung oder Vernichtung sensibler Informationen gewährleistet sein.

### Regeln einhalten

Verantwortliches Handeln heißt auch, sich an Regeln zu halten. In diesem Zusammenhang spielt das Thema Compliance eine große Rolle. Das bedeutet, Unternehmen müssen gesetzliche Regeln erfüllen und sollten zusätzlich freiwillige Vorschriften einhalten. Beispielsweise schreibt der Gesetzgeber vor, dass Informationen eine bestimmte Zeit aufbewahrt werden müssen. Dabei sind Datensicherheit und -schutz entscheidend. Compliance geht jedoch über Datenspeicherung hinaus, sie umfasst auch das Datenmanagement. So müssen Unternehmen Archivierungsregeln aufstellen und für die Sicherheit, Integrität und Auffindbarkeit der Informationen sorgen. Wichtig dabei ist eine Strategie, die Menschen, Prozesse und Technologien einbezieht.

Welche Folgen es haben kann, wenn die betroffenen Abteilungen in Bezug auf Datenschutz nicht zusammen arbeiten, verdeutlicht eine entsprechende Studie („Microsoft Study on Data Protection and Role Collaboration Within Organizations“), die das Ponemon Institute LLC im Oktober 2007 in den USA, Großbritannien und Deutschland durchgeführt hat. Kernergebnis: Drei Viertel der befragten Unternehmen, bei denen kaum eine Kooperation stattfand, verzeichneten in den vergangenen 24 Monaten einen oder mehrere Datenmissbräuche. Vor allem muss die Kommunikation zwischen denjenigen, die Daten sammeln und den Sicherheits- und Datenschutz-Experten stimmen. Das ist jedoch in Unternehmen nur selten der Fall. Lediglich ein Drittel der Marketing-Mitarbeiter tauscht sich mit den Sicherheitsexperten über die Datensammlung und -nutzung aus.

### 2.2 | Microsoft: Datenschutz als Unternehmensgrundsatz

Datenschutz ist für Microsoft seit Langem ein wichtiges Thema. Neben Sicherheit, unternehmerischer Integrität und der Zuverlässigkeit von Software, Diensten und Produkten bildet es die vierte Säule der Trustworthy Computing Strategie, die 2002 von Bill Gates als oberster Unternehmensleitsatz formuliert wurde. Im Bereich des Datenschutzes gilt dabei

der Grundsatz: Sicherheit geht vor Funktionalität – und zwar bei der Entwicklung aller Microsoft-Produkte und -Services. Die so geschaffenen Lösungen sollen den Anwendern helfen, vertrauensvoll mit den digitalen Medien umzugehen und sich vor Datenmissbrauch zu schützen.

### **Klare Richtlinien für die Produktentwicklung**

Microsoft hat in den vergangenen Jahren seine internen Datenschutzrichtlinien für die Bereiche Vertrieb und Marketing sowie Entwicklung stetig verbessert. So gilt beispielsweise bereits seit 2005 im Unternehmen das Prinzip des Security Development Lifecycle (SDL), in das Datenschutzstandards für die Softwareentwicklung integriert wurden. So achten alle Microsoft-Entwickler von Anfang an darauf, dass neue Software und Services datenschutzkonform sind – und zwar über den gesamten Produktlebenszyklus hinweg.

Ein Ziel dabei ist es, den Verbrauchern die Kontrolle über ihre persönlichen Informationen zu geben. Sie sollen genau wissen, welche Daten gesammelt, an wen diese verteilt und wie sie verwendet werden. Ohne ihr Einverständnis werden beispielsweise keine persönlichen Informationen von ihrem Computer übertragen. Auch haben die Anwender jederzeit Zugriff auf ihre Daten und können diese bearbeiten. Die Microsoft Datenschutzstandards sind zudem öffentlich zugänglich. So können auch freie Entwickler ihre Anwendungen entsprechend anpassen.

Seine Datenschutzrichtlinien entwickelte Microsoft auf Basis der Datenschutz-Leitlinien der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) sowie der Datenschutzrichtlinie der Europäischen Union. Darüber hinaus setzt sich Microsoft für weltweit gültige Datenschutzrichtlinien bei der Software- und Serviceentwicklung ein. Politik, Unternehmen und Wissenschaft sollten diese gemeinsam erarbeiten. Ein Beispiel: Microsoft engagiert sich in der International Association of Privacy Professionals (IAPP). Mehr als 4.000 Datenschutzexperten aus 32 Ländern haben sich in diesem Verband zusammengeschlossen. Ihr Ziel ist es, den Austausch und die Weiterbildung im Bereich Datenschutz zu fördern.

Außerdem ist Microsoft Mitglied des TRUSTe Privacy Seal Program und der Network Advertising Initiative (NAI).

### **Gütesiegel bescheinigen Qualität**

Dass Microsoft die Datenschutzanforderungen erfüllt, belegen auch Datenschutz-Siegel für Microsoft-Produkte. Diese Qualitätszeichen werden von unabhängigen Prüfstellen, wie dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD), verliehen. Beispielsweise hat die Anwendung Windows Genuine Advantage (WGA) Version 1.7 für Windows XP ein Gütesiegel vom ULD erhalten. Diese Anwendung überprüft, ob auf Computern autorisierte Software-Lizenzen laufen. So weiß der Nutzer, ob sein Windows XP legal ist und damit den Sicherheitsanforderungen von Microsoft entspricht. Die Einhaltung des Datenschutzes beim Windows Update Service wurde ebenfalls vom ULD mit einem Gütesiegel bescheinigt.

Eine Weiterführung des Gütezeichens auf europäischer Ebene ist das European Privacy Seal (EuroPriSe): Es prüft die Einhaltung europäischer Datenschutzrichtlinien. Neun Partner aus acht EU-Mitgliedsstaaten wollen unter der Leitung des ULD mit EuroPriSe einen europäischen Standard für die Bewertung von IT-Produkten und IT-basierten Services schaffen. Wer das Siegel erhalten möchte, muss einen zweistufigen Evaluationsprozess durch unabhängige Experten durchlaufen. Das Pilotprojekt läuft bis November 2008.

### **2.3 | Suchmaschinen und Online-Werbung: anonym surfen**

Gemeinsam mit qualifizierten Partnern entwickelt Microsoft auch den Datenschutz bei Suchmaschinen und Online-Werbung weiter. Ziel ist es, einen offenen Dialog mit anderen Unternehmen, Wissenschaftlern und Verbraucherschützern anzustoßen – und international gültige Rahmenbedingungen zu schaffen.

Den Datenschutz bei Bing hat Microsoft bereits deutlich verbessert. Vor allem bei der Personalisierung der Suchdienste: Die Nutzer haben mehr Kontrollmöglichkeiten darüber, welche Informationen verwendet werden, damit die Online-Services auf ihre Bedürfnisse zugeschnitten sind. Für die Weiterentwicklung und Verbesserung von Bing erhebt Microsoft auch Daten über die Anwender und ihr Verhalten. Diese Informationen können jedoch anonym bleiben. Das bedeutet, es gibt keinerlei Verbindung oder Verlinkung, die Rückschlüsse auf den einzelnen Nutzer zulässt. Microsoft hat folgende Regeln für den Schutz der Privatsphäre bei der Online-Suche und -werbung aufgestellt:

- Datenschutzrichtlinien müssen transparent und leicht verständlich sein. Nur so können die Nutzer bewusste Entscheidungen treffen. Die Microsoft Online-Datenschutzerklärung wird regelmäßig aktualisiert und ist von den meisten Webseiten zugänglich.
- Die Nutzer sollen die Kontrolle behalten. Beispielsweise können sie genau bestimmen, welche Informationen sie von Microsoft erhalten möchten. Dazu gehören unter anderem Opt-out-Möglichkeiten bei Werbeanzeigen.
- Suchanfragen sind getrennt abgelegt von Informationen, die den Nutzer eindeutig identifizieren würden. So wird verhindert, dass diese Daten ohne Zustimmung der Nutzer miteinander verbunden werden können.
- Daten aus der Suche mit Bing werden nach 6 Monaten vollständig gelöscht. Dies umfasst das endgültige Entfernen von Cookies, der gesamten IP-Adresse und anderer Identifizierungsmerkmale. Bei der Datenspeicherung für personalisierte Suchanwendungen müssen die Nutzer den Bedingungen zustimmen.

## 2.4 | Privatanwender: Sicheres Verhalten fördern

Mit Windows Vista hat Microsoft den Schutz der Anwender weiter erhöht. Es ist das erste Betriebssystem, das von Anfang an nach dem Prinzip des Security Development Lifecycle (SDL) entwickelt wurde.

Sicherheit hat demnach oberste Priorität. So aktiviert Windows Vista unter anderem automatisch die Firewall und ruft Updates auf. Der PC ist damit immer gut geschützt. Eltern haben außerdem die Möglichkeit, spezielle Jugendschutzeinstellungen vorzunehmen. Ihr Nachwuchs kann dann beispielsweise auf keine Seiten mit pornografischen Inhalten oder Glücksspielangeboten klicken und nur vorher festgelegte Spiele aufrufen.

## Digitale Identitäten verwalten

Eine weitere Funktion von Vista ist Windows CardSpace. Diese Anwendung vereinfacht und verbessert die Identitätskontrolle im Internet. Der Anwender erstellt eine oder mehrere virtuelle Karten mit persönlichen Informationen oder lässt sich diese beispielsweise von seiner Bank oder einem Online-Shop ausstellen. Windows CardSpace verwaltet die digitalen Identitäten – ähnlich wie eine Brieftasche, in der mehrere physische Karten stecken. Der Nutzer verwendet dann die Karte mit den für eine Anwendung relevanten Informationen. Beispielsweise Name, Adresse und Zahlungsinformationen, wenn er online einkauft. Windows CardSpace basiert auf offenen Kommunikationsstandards und unterstützt unterschiedliche Software auf allen Plattformen.

## Privatsphäre wahren

Mehr Sicherheit und Datenschutz im World Wide Web bietet der Internet Explorer 8. Er unterstützt das sichere und anonyme Navigieren auf Internetseiten. Mit der optionalen Funktion „InPrivate-Browsen“ bleibt der Nutzer unerkannt. Der Browserverlauf, temporäre Internetdateien, Formulardaten, Cookies, Benutzernamen und Kennwörter werden nicht gespeichert. So gibt es auf dem genutzten PC keinerlei Spuren und Hinweise auf Suchverlauf und Surfverhalten. Weitere Sicherheitskomponenten des Internet Explorer 8 sind der SmartScreen-Filter, mit dem Microsoft das Erkennen von Phishingseiten verbessert sowie eine Funktion, die auf manipulierte Webseiten hinweist.

## Medienkompetenz trainieren und Jugend schützen

Innovative Technologien sind eine Möglichkeit, die Privatsphäre der Anwender zu wahren. Doch auch die Nutzer sollten ein stärkeres Bewusstsein für den Schutz ihrer Daten entwickeln. Gerade im Internet handeln viele sorglos. In sozialen Netzwerken wie StudiVZ, Facebook oder Xing geben sie oft sehr persönliche Daten preis. Den Anwendern fehlt häufig das Wissen darüber, was mit diesen Daten geschieht und wer Zugang dazu hat. Ihnen ist meist nicht bewusst, dass sie die Datenschutzeinstellungen in ihrem System oder ihrem Browser in der Regel selbst vornehmen müssen.

Microsoft unterstützt deshalb Initiativen, die den Nutzern sicheres Verhalten im Internet vermitteln. Denn wie im realen Leben auch, müssen die Nutzer lernen, möglicherweise gefährliche Situationen auch online zu erkennen und angemessen zu reagieren. Mit dem Internet Risk Behaviour Index, kurz IRBI, hat Microsoft gemeinsam mit Wissenschaftlern der Münchner Ludwig-Maximilians-Universität (LMU) erstmals eine realitätsnahe Simulation riskanter Online-Situationen, darunter Datenschutz-Szenarien, entwickelt. Seit Juni 2008 können Nutzer ihr sicherheitsrelevantes Verhalten auf [www.irbi.de](http://www.irbi.de) trainieren und verbessern. Sie spielen typische Gefahrensituationen – etwa den Software-Download aus einer nicht vertrauenswürdigen Quelle – am Bildschirm durch. Für die Bewältigung der Aufgaben erhalten die Nutzer Punkte, die sich zum Internet Risk Behaviour Index addieren. Je nachdem, wie die Nutzer abschneiden, bietet Microsoft ihnen online Hilfestellungen an.

Um schon bei jungen Nutzern ein stärkeres Bewusstsein für Sicherheit und Schutz der Privatsphäre im Web herzustellen, hat Microsoft die Initiative „Sicherheit macht Schule“ ([www.sicherheit-machtschule.de](http://www.sicherheit-machtschule.de)) gegründet. Sie dient als Forum für Unterrichtsideen, in dem Lehrer, Eltern und andere Verantwortliche Anregungen erhalten, wie sie Kinder und Jugendliche zu umsichtigem Verhalten anleiten können. Beispielsweise üben sie mit den Schülern, welche Passwörter sicher sind und wie sie selbst ein starkes Passwort auswählen. Weitere Initiativen wie

die Internauten ([www.internauten.de](http://www.internauten.de)) und klicksafe ([www.klicksafe.de](http://www.klicksafe.de)) vermitteln den Kindern und Jugendlichen, wie sie sich im Internet richtig verhalten und Risiken vermeiden können.