

Konsumentenschutz
Prinz-Eugen-Straße 20-22
A-1041 Wien
Tel: ++43-1-501 65/2144 DW
E-Mail: konsumentenpolitik@akwien.at



07/2009
Februar 2009

PRIVATSPHÄRE IN BEDRÄNGNIS

Neue Herausforderungen für Verbraucher- & Datenschutz

Daniela Zimmer

Die wichtigsten Ergebnisse

- **ÖsterreicherInnen hinterlassen von Jahr zu Jahr mehr Datenspuren. Allein 25 der geläufigsten privaten und öffentlichen Datenverwender speichern insgesamt bis zu 40 verschiedene Datenarten über eine einzelne Person:**
- Öffentliche Organisationen verarbeiten zwar in der Regel noch mehr Daten als Private. Allerdings holen private Institutionen auf.
- Bei Arbeitgebern, Finanzdienstleistern und Telekom- bzw Internetanbietern ist die anfallende Datendichte besonders groß.
- Wachsenden Datenhunger zeichnet Wirtschaftsauskunfteien, Adressverlage und auch manche Webshops aus.
- Vor allem bei Web 2.0 Plattformen wie Facebook und Suchmaschinen-Betreiber fällt massenhaft Datenmaterial an – bestens geeignet für Personenprofile.
- Hinzukommen neue Datenkategorien wie etwa Bilddaten durch den Videoüberwachungs-Boom und biometrische Daten, wie etwa den Fingerprints in Pässen.

Die Privatsphäre gerät bei so viel Datensammelwut in Bedrängnis

“Was einmal privat war, ist nun öffentlich

Was einmal schwierig zu kopieren war, ist nun ganz einfach zu vervielfältigen.

Was einmal leicht vergessen worden ist, wird nun ewig gespeichert.“

(Ronald Rivest, einer der Entwickler des RSA-Verschlüsselungsverfahrens)

Die AK hat eine Studie bei der Akademie der Wissenschaften, Institut für Technikfolgen-Abschätzung, in Auftrag gegeben. Die Studie zeigt, dass der Zug aus Sicht des Datenschutzes weiter in die falsche Richtung fährt

- Es wird zu viel gespeichert, das die Privatsphäre unverhältnismäßig beeinträchtigt
- Wer was wozu wie lange speichert, ist für den Einzelnen nicht mehr überschaubar
- Datenschutzverstöße bleiben lange unentdeckt. In Deutschland berichteten Medien zB über gravierende, aber zum Teil lange zurückliegende Datenschutzverstöße (zB heimliche, exzessive Mitarbeiterkontrolle zu Antikorruptionszwecken bei der deutschen Bahn vor sechs Jahren). Der Datenmissbrauch ist verantwortlichen Stellen oft bekannt, ohne dass die Betroffenen oder die Datenschutzbehörde darüber informiert werden. So können Sicherheitsmaßnahmen nicht rechtzeitig ergriffen und Schäden begrenzt werden.
- Hilfsmittel gibt es (Datenschutz-Gütezeichen, Privacy-Software uä). Sie werden aber zuwenig genutzt, sagen die AK-Konsumentenschützer.
- Der Verlust an Selbstbestimmung über eigene Daten und Privatsphäre erfolgt schleichend und löst Gewöhnungseffekte aus. Information und Bewusstseinsbildung sind deshalb wichtig. Sie reichen aber allein nicht:

So geben zB Studenten, die soziale Internet-Netzwerke wie zB Facebook nutzen, in einer Salzburger Befragung aus 2009 an, dass sie Datenschutzverstöße der Plattformanbieter vermuten, aber ihr Nutzungsverhalten deshalb nicht ändern werden.

Die AK-Konsumentenschützer fordern deshalb ua.

- eine gesetzliche Infopflicht bei Datenschutzpannen: Datenverwender müssen Betroffene und die Datenschutzbehörde über schwerwiegende Vorfälle (Missbrauch, Verlust, Diebstahl von Daten und drohenden Sicherheitsrisiken) informieren.
- Entwicklungen, die die Privatsphäre stark gefährden können (Videoüberwachung, RFID) sind restriktiv zu regeln.
- Strenge Anforderungen an den Datenschutz in Betrieben und betriebliche Datenschutzbeauftragte
- mehr Schutz für Verbraucher vor unerbetenen Werbeanrufen und eine ausdrückliche Zustimmung zur Datennutzung, wenn dem Verbraucher per Telefon, SMS, Fax oder E-Mail Werbung zugehen soll.

- „Internetdaten mit Zeitablauf“: Internetnutzer müssen Zugriff auf selbst im Internet veröffentlichte Daten haben (um sie zB löschen zu können)
- mehr Ressourcen für Datenschutz-Kontrollen
- vorbildliches Datenschutzverhalten muss sichtbar werden. Nicht jede Datensammlung kann von Datenschützern kontrolliert werden, deshalb braucht es Anreize, dass Datenverantwortliche Datenbanken, IT-Sicherheitssysteme etc. freiwillig testen lassen. Dafür gibt es ein Gütezeichen (zB das Europäische Datenschutzgütesiegel EuroPriSe und einen öffentlichen Imagegewinn. Deutschland ist Vorreiter – Österreich sollte nicht hinterhinken.

Übersicht über Datenspuren der DurchschnittsösterreicherInnen

Legende zur Tabelle auf Seite 4:

Mit einem „X“ markierte Felder stehen für Daten, die mit Sicherheit oder sehr hoher Wahrscheinlichkeit gespeichert werden; die mit einer „0“ gekennzeichneten Felder für Daten, die möglicherweise bzw. mit geringer Wahrscheinlichkeit gespeichert werden; weiße Felder ohne Markierung signalisieren, dass die jeweiligen Daten vermutlich nicht gespeichert werden.

Zum Vergleich: Datenspuren der DurchschnittsösterreicherInnen im Jahr 2000

Daten		Institution/Organisation	Öffentlich										Privat						
			Meldewesen	Grundbuch	Kommunale Verwaltung	Polizei/Gericht	Bundesheer/Zivildienst	Finanzbehörden	Sozialversicherung	Gesundheitssystem	Bildungssystem	Statistik Österreich (Volksz.)	Arbeitgeber	Finanzdienstleister	Telekommunikation	Kirchen	Private Versicherungen	Rundfunk, Medien	Vereine
Standard Grunddaten	Name (Vor- und Nachname)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Geschlecht	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Titel	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Postadresse	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Erweiterte Grunddaten	Telefonnummer (Festnetz-Mobil, frei verfügbar)			0	0	0	0	0	0	X		X	0	X	0	0	0	0	0
	Telefonnummer (Festnetz geheim, Wertkartenhandy)									0			X						
	Faxnummer			0	0	0	0	0	0		0	0	0	X		0	0	0	0
	Email-Adresse				0							0	0	X		0	0	0	0
Private Lebenslaufdaten	Geburtsdatum/Alter	X	X	X	X	X	X	X	X	X	X	X	0	X	X	X	0	0	0
	Geburtsort	X			0	X				X	X	0		X					
	Familienstand			X	0	X	X	X	X	X	X	X	0		0	X	0	0	0
	Staatsangehörigkeit	X	0	X	X	X	X	X	X	X	X	X	0	0	0	X	0	0	0
	Beruf				0	X	X	X	0	X	X	X	0	0	0	X	0	0	0
	Arbeitsstätte				0	0	X	X	X	X	X	X	X	X		X			
	Anzahl Kinder			X		0	X	X	X	X	X	X	0		0	X			0
	Bildungsweg					X	X	X	X	X						0	0		0
	Konfession	X				X						0			X				
Privatleben	Daten über Familienangehörige (Name, Adresse, Beruf etc.)			X		X	X	X	X	X	0	X	0	X	X				0
	Wohnungsgröße			0							X		0		X				
	Mitbewohner/innen / zum Haushalt gehörende Personen						0	0			X								
	Nachbarn										X								
Versicherung	Sozialversicherungsnummer				0	X	X	X	X			X				0			
	Versicherungsdaten (Lebens-, Kranken-, Autoversicherung etc.)						X	X	X			0			X				
Körper	Gesundheits-/Krankheitsdaten				0	X	0	X	X			0			0				
	DNA-Daten				0				0										
Finanzielle Daten	Bankdaten (Konto-, Kreditkartennummer; Kontostand)					X	X	0				X	X	X	0	X	X	0	0
	Einkommen						X	X				X	X		0	0			0
	Ausgaben											X							0
	Bonität						X					X	X	X	0				
	Gezahlte Steuern						X					X	0						
Vermögen	Immobilien		X				X					X							
	Sonst. nicht-monetäres Vermögen						0					0			X				
Kriminalität	Kriminaldaten / polizeilich gespeicherte Daten				X	0						0							
Kontakte	Geschäftliche Kontakte (Zeitpunkt, Häufigkeit, Dauer, Medium, Ort)											X		X					
	Private Kontakte (Zeitpunkt, Häufigkeit, Dauer, Medium, Ort)												X						0
Gewohnheiten	Bewegungsdaten				0							0	X						
	Freizeitverhalten													0				0	0
	Einkaufsverhalten												X	0					X
	Benutze Internetseiten/persönliche Vorlieben													X			0	0	0
	Politische Einstellungen und Interessen					0	0										0		0

X = Daten werden mit sehr hoher Wahrscheinlichkeit registriert bzw. gespeichert, 0 = Daten werden möglicherweise/mit geringer Wahrscheinlichkeit registriert oder gespeichert, (leeres Feld) = Daten werden mit hoher Sicherheit nicht gespeichert

Die AK-Studie beschreibt die größten Herausforderungen für den Schutz der Privatsphäre

▪ **Die rasante Entwicklung von Kommunikations- und Informationstechnik**

Neue Technologien erleichtern und verbilligen das Anlegen und Auswerten gewaltiger Datenmengen. Sie vervielfachen auf diese Weise die Datenspuren, die KonsumentInnen bewusst oder auch unbemerkt hinterlassen. Trends mit teils gravierenden Auswirkungen auf die Privatsphäre verbreiten sich so rasch, dass Datenschutzmaßnahmen den Entwicklungen weit hinterher hinken. Datenschutzfördernde Technologien werden umgekehrt in der Praxis wenig genutzt. Folgende Entwicklungen können die Privatsphäre intensiv berühren:

- Durch die Verbilligung rechenstarker Computer und Datenspeicher ist die Speichermenge nahezu unlimitiert
- Funkchips, die Barcodes ablösen und über Lesegeräte Personen und Sachen identifizieren (RFID)
- Web 2.0, das Social Network Webseiten, Geotagging, Wikis, Blogs u.ä ermöglicht
- „Überall Kommunikation“ – Google Earth bzw Street View bieten Internet-Rundumsichten von Gebieten und Straßen. Dazu wird vom Auto aus auch in Häuser hineingefilmt, werden Autokennzeichen erfasst uä. Google Latitude soll angemeldeten Mitgliedern einer Gruppe ermöglichen, untereinander den momentanen Standort zu orten. Ideal auch für Hobbyspione: Personenortungsdienste via GPS und Handy.
- Sensortechnik, mit deren Hilfe nicht nur Autokennzeichen gescannt werden können, sondern mittels Video-Analyse-Software auch das (definiert auffällige) Verhalten von Menschen auf öffentlichen Plätzen
- Das Handy als zentrale Drehscheibe für Dienste zur Bezahlung, als Navigationssystem, elektronisches Ticket, Einstieg ins Internet usw. verschafft Mobilfunkanbietern massenhaft Datenmaterial.

▪ **Die fehlende Transparenz über Verarbeitungsvorgänge (wer speichert und übermittelt was wofür)**

Die Anzahl der Datensammlungen allein bedroht den Datenschutz gar nicht so sehr. Erst durch die zunehmende Vernetzung, Firmenfusionen, die Auslagerung von Tätigkeiten, Datenauswertungsprogramme uä sind umfassendere Aussagen über Einzelpersonen möglich, als sich aus den einzelnen Datensätzen allein ergäbe.

▪ **Die fehlende Transparenz bei Datenschutzpannen**

Datenschutzskandale, wie in Deutschland oder Großbritannien aufgedeckt (der deutschen Telekom wurden zB 17 Millionen Kundenstammdaten entwendet; britische Behörden verloren Datenträger mit Millionen Daten von Kindergeldempfängern) zeigen, dass Datenschutzverstöße und unzureichende Datensicherheit eher zufällig aufgedeckt werden. Betroffene erfahren nicht oder zu spät von Vorfällen - und können sich nicht rechtzeitig vor den Folgen schützen.

- **Der Trend zu Kundenbewertung**
 KonsumentInnen werden von Banken, Versicherungen, Telekomunternehmen und dem Versandhandel eingehenden Risiko- und Verhaltensanalysen unterzogen, um Prognosen zu erstellen. Wird ein Kunde bspw. rentabel und ein pünktlicher Zahler sein? Bonitätschecks entscheiden darüber, ob KonsumentInnen als Vertragspartner akzeptiert werden. Ist diese Hürde genommen, entscheidet die Schublade mit der Aufschrift „Kundenklasse“ oft auch über die Konditionen, die Unternehmen gewähren. Die Gefahr, dass Intransparenz über diese Vorgänge, überschießende Datennutzungen und wissenschaftlich fragwürdige Bewertungsmethoden den Verbraucher im Geschäftsleben benachteiligen, wächst.
- **„Mitmach - Web“**
 My Space und Facebook verwalten die Profile von jeweils (!) 140 bzw.180 Millionen Nutzern. Auf sozialen Netzwerkseiten nicht eingetragen zu sein und keine „Freunde zu sammeln“ ist für viele Jugendliche fast unvorstellbar, der soziale Druck mit eigenem Nutzerprofil für sich zu werben und interaktiv zu sein, wächst. Das lustvolle Kommunizieren im Web wird von der irrigen Vorstellung begleitet, dass man sich zwar halb-öffentlich aber doch im Freundeskreis austauscht. Im Gegensatz zum Austausch am Wirtshausstammtisch bleiben Webeinträge aber dauerhaft abrufbar und können, wenn Sicherheitseinstellungen nicht genutzt, unterlaufen oder erst gar nicht angeboten werden, für Personenprofile genutzt und weiterverkauft werden. Berichte über Personalbüros, die sich Webeinträge über Jobbewerber standardmäßig „ergoogeln“, belegen, wie zweischneidig Offenherzigkeit im Internet ist.
- **Überwachte Mitarbeiter**
 Mitarbeiter, die beim deutschen Discounter Lidl exzessiv überwacht wurden, die Deutsche Bahn, die rund 173.000 Mitarbeiter im Zuge eines Datenabgleichs heimlich auf Korruption überprüft hat -Fälle wie diese zeigen, dass die in Betrieben genutzte Technik (IKT, Videokameras) sehr leicht für überschießende Kontrollzwecke missbraucht werden kann.
- **fehlendes Datenschutzbewusstsein**
 Die Wichtigkeit von Privatsphäre anerkennt prinzipiell jeder. In der Praxis steht das Verhalten von Unternehmen, Behörden aber auch den KonsumentInnen selbst oft im krassen Widerspruch dazu: Im Internet werden über soziale Netzwerkseiten intimste Details freiwillig veröffentlicht, für Gewinn- oder Rabattversprechen geben KonsumentInnen eine Vielzahl an persönlichen Daten für Marketingzwecke preis. Unternehmen verwenden in ihren Geschäftsbedingungen Datenschutzerklärungen, die in Wahrheit keine Beschränkungen enthalten sondern ihre Datensammelwut belegen. Anspruch und Wirklichkeit decken sich auch nicht im Sicherheitsbereich: die Privatsphäre gerät gegenüber Überwachungsinteressen oft schon ins Hintertreffen, bevor noch geklärt ist, wie wirksam und angemessen Kontrollmaßnahmen überhaupt sind.

- **Videüberwachung**

Ob Verkehrsbetriebe, Hausverwaltungen, Geschäftsbesitzer – Private Videoüberwachung wird als Allheilmittel zur Abschreckung und Deliktsaufklärung genutzt. Experten warnen aber, dass der erhoffte Effekt selten erreicht wird (unerwünschtes Verhalten wird nur räumlich verdrängt, Täter setzen Maskierungen ein etc) Sicher ist nur, dass die so überwachte Gesellschaft Freiheitsrechte aufgibt. Erweist sich Videoüberwachung für die angegebenen Zwecke als ungeeignet, ist sie unverhältnismäßig und damit eigentlich unzulässig. Alternativen gibt es fast immer - sie gelten aber oft als zu teuer: mehr Mitarbeiter als Sicherheitskontrolle oder im Einsatz gegen Vandalismus; Echtzeitüberwachung über Monitore ohne Datenspeicherung. Weitere Kritik: viele private Videokameras sind ohne nötige Genehmigung durch die Datenschutzkommission im Einsatz und mangels Kennzeichnung oft nicht erkennbar.

- **Schwächung des Datenschutzes auf EU-Ebene**

- **zB Fluggastdaten:** die Weitergabe von Passagierdaten vor Abflug an das US-Heimatschutzministerium, das riskante Fluggäste ausfiltern kann, bevor die Maschine startet, ist unter Dach und Fach. Nun plant die EU-Kommission - begleitet von Kritik des EU-Parlaments und Datenschützern - ein vergleichbares System in Europa.

- **zB Vorratsdatenspeicherung von Telefon- und Internetverkehrsdaten:** Die EU-Richtlinie über Vorratsdatenspeicherung aus 2006 warf aus Anlass der Terrorbekämpfung die Datenschutzgarantie über Bord, wonach Verkehrsdaten spätestens nach Abrechnung der Entgelte gelöscht werden müssen und ordnet eine verdachtsunabhängige Speicherung aller Daten an. Vom Datenhorten wird jeder Konsument, der Telefon, Handy oder Internet benutzt, betroffen sein. Verkehrsdaten, also wer mit wem, wann, wie lange telefoniert hat, auch der Standort von Handy-Anrufern und der Ursprung und das Ziel einer Internetverbindung sollen zumindest sechs Monate aufgehoben werden. Mit richterlichem Beschluss können Behörden auf die Daten zugreifen. Die Richtlinie ist in Österreich noch nicht umgesetzt.

- **die zunehmende Internationalisierung der Datenflüsse**

Kunden- und Mitarbeiterdaten fließen von Tochterunternehmen zu Konzernmüttern zB in die USA oder die Verwaltung von Datenbanken wird nach Indien ausgelagert. Vertragliche Datenschutzgarantien zählen wenig, wenn eine Kontrolle vor Ort praktisch unmöglich ist. Die Unterschiede zwischen dem gesetzlichen Datenschutzniveau in Drittländern und der EU, aber auch der historisch gewachsene Stellenwert der Privatsphäre unter den einzelnen EU-Mitgliedsländern könnte zum Teil größer nicht sein.

- **Mit Funkchips vom anonymen Konsumenten zum erfassten Kunden**

Mit einem Lesegerät können Personen und Sachen, die einen Funkchip tragen, identifiziert werden. Die Funkchips ersetzen Barcodes bzw Magnetstreifenkarten und werden in der Lagerlogistik und bei der Rückverfolgung der Herkunft von Waren (Lebensmitteln, Arzneien) genutzt, aber auch bei Tickets, die berührungslos auslesbar sind (bei Schiliften, Verkehrsbetrieben uä). Die Chips zu Spottpreisen können alle Handelswaren zieren, Patienten auf Armbändern im Spital begleiten u.v.m. Zu den Gefahren zählen: über Entfernung auslesbare Informationen können von Unbefugten mitgelesen werden. Kundenverhalten kann (in Verbindung mit Kreditkarten- oder Kundenkarten) studiert werden.

- **Der Druck zu effizienterer Verwaltung**

In den kommenden Jahren soll bspw der elektronische Gesundheitsakt kommen, um den Wissensaustausch im Gesundheitssystem zu verbessern. Nach aktuellem Plan soll der Patient entscheiden, ob und welche Daten gespeichert werden und wer Zugriff darauf haben soll. Fraglich ist, welche Nachteile Patienten ohne elektronischen Krankenakt in der Praxis haben werden. Versicherungen und Arbeitgeber könnten beginnen, auf eine Preisgabe der elektronisch gesammelten Daten zu drängen.

- **Datenschürfen im Internet**

- Jeder Klick im Internet ist an eine Internet-Adresse geknüpft. Wer an Interessensprofilen interessiert ist, muss gar nicht auf die Log-Files der Internetprovider zugreifen. Viele Seitenanbieter gebrauchen "Cookies" (über diese Files werden nutzerbezogene Daten auf der PC-Festplatte des Konsumenten gespeichert). Sie erleichtern den Surfaltag (sie automatisieren Routineeingaben, merken sich bestellte Artikel in einem Warenkorb usw.), vereinfachen aber auch das Erstellen von Nutzerprofilen.
- Der Polizei ist nun auch erlaubt, bei Gefahr in Verzug ohne richterliche Anordnung (mit Hilfe der Provider) Handystandort-Daten zu ermitteln und Auskunft über Name, Anschrift und Teilnehmernummer zu einer bestimmten IP-Adresse zu verlangen. Die Polizei hat allein zwischen Jänner und April 2008 3.863-mal Auskunft zu IP-Adressen verlangt.

AK-Forderungen

Die AK-Studie stellt fest, dass in vielen Bereichen der Datenhunger wächst. Die allgemeinen Regeln des Datenschutzgesetzes reichen nicht immer aus:

Die Datennutzung an eine Zustimmung des Verbrauchers zu binden, hilft nichts, wenn der Verbraucher in der Praxis ohne sein OK zur Datennutzung an manchen Diensten nicht teilhaben kann. Daten dürfen gesammelt werden, wenn ein Gesetz es ausdrücklich erlaubt, der Betroffene zustimmt oder ein „überwiegendes, berechtigtes Interesse“ an der Datennutzung gegenüber dem Geheimhaltungsinteresse besteht. Wann Letzteres zutrifft, darüber kann im Einzelfall intensiv gestritten werden.

Für die AK-Konsumentenschützer sind deshalb in datenschutzsensiblen Bereichen „gesetzliche Appetitzügler“ erforderlich: denn Datenvermeidung ist der beste Schutz. Daher verlangen die AK-Konsumentenschützer:

...für den privaten bzw kommerziellen Bereich

- **Informationspflicht bei gravierenden Datenschutzpannen:** haarsträubende Vorfälle wie in England und Deutschland gab es erfreulicherweise in Österreich noch nicht. Datenmissbrauch und –sicherheitsprobleme können aber vorkommen. Eine Verständigungspflicht gegenüber Datenschutzkommission und Betroffenen fehlt in Österreich. Nur informierte Betroffene können Schritte zur Schadensvermeidung setzen und eventuell Schadenersatz fordern. Etliche Staaten haben bereits entsprechende Regelungen. Sie schaffen Transparenz und mehr Vertrauen in den korrekten Umgang mit ihren Daten und halten Unternehmen und Behörden dazu an, mehr in Datenschutz und Datensicherheit zu investieren.
- **Unerwünschte Werbeanrufe** verletzen die Privatsphäre auf penetrante Weise und dürfen nicht überhandnehmen. Derzeit sind Vertragsabschlüsse durch „Cold Calling“ überaus lohnend, deshalb sind höhere Strafen bzw Gewinnabschöpfung notwendig. Verträge die auf diese Weise zustande kommen sollten (schwebend) unwirksam sein.
- **Ausdrückliche Zustimmung zur Nutzung von Mailadresse, Rufnummer für Marketingzwecke:** Verbraucher übersehen häufig Datenschutzklauseln in Geschäftsbedingungen. Die Klauseln sind abgesetzt von AGB-Fließtexten hervorzuheben. Bei Datennutzungen, die die Privatsphäre besonders intensiv berühren (zB die Verwendung von Mailadresse oder Rufnummer für Marketingzwecke) sollte der Konsument nur durch einen aktiven Schritt (zB Ankreuzen, Unterschrift) sein Einverständnis erteilen können. Dies entspricht einer Angleichung an deutsche Datenschutzstandards (BGH Payback Entscheidung Az: VIII ZR 348/06 vom 16. Juli 2008).

Auch die kommerzielle Verwertung von Daten aus Internetdiensten durch Dritte sollte die ausdrückliche Zustimmung der NutzerInnen voraussetzen. Die Verweigerung dieser Zustimmung darf nicht zum Ausschluss vom Dienst führen.

- Schutz vor „ewigen“ unlöschbaren Einträgen im Internet, zB auf **sozialen Netzwerkseiten**: einmal veröffentlicht – nie mehr getilgt: der Plattformanbieter entscheidet was an selbsterzeugten Inhalten im Mitmach-Web gelöscht werden kann. Nötig sind spezifische Lösungsrechte (zB gesetzliche Fristen, innerhalb der Alteinträge zu löschen sind) und Grenzen für die Verwertung veröffentlichter Daten im Internet (zB Datensammlungen in Suchmaschinen wie zB www123people). Betreiber von Web 2.0-Plattformen sollten die individuell nutzbaren Sicherheitseinstellungen verbessern.

- **Stärkerer betrieblicher Datenschutz**
Die Durchsetzung von Datenschutzbestimmungen in der Arbeitswelt muss deutlich verbessert werden. Vorfälle wie in Deutschland (Exzessive Mitarbeiterüberwachung bei Lidl, deutsche Telekom und Bahn) sind abschreckende Beispiele. Die Datenschutzerfordernisse in Betrieben mit moderner IKT-Ausstattung sind so komplex, dass es zB der Expertise und Kontrolle durch einen weisungsfreien betrieblichen Datenschutzbeauftragten braucht.

- **Bessere Auskunftsrechte gegenüber Datenverarbeitern**
derzeit berufen sich Auskunftspflichtige gerne darauf, dass bezüglich der Herkunft der Daten einfach keine Informationen (mehr) verfügbar sind. Explizite Protokollvorschriften sollten den Betroffenen in diesen Fällen auch zu einer Auskunft über die Datenquelle verhelfen.

- **Videoüberwachung**
 - Zulässigkeit nur bei über das gewöhnliche Maß hinausgehenden, besonderen Gefährdungslagen;
 - Verhältnismäßigkeitstest – Nachweis, weshalb schonendere Mittel (Alarmanlage, Aufsichtspersonen, Echtzeitüberwachung etc.) nicht ausreichen;
 - Einsatz für Zwecke der Beweismittelsicherung nur aufgrund rechtmäßiger Datenermittlung; als Primärzweck nur für die Durchsetzung von Ansprüchen, die dem Grundrechtseingriff zumindest gleichwertig sind;
 - Spezielle, äußerst restriktive Regelungen für Videoüberwachung am Arbeitsplatz (zB Nachweis bei Echtzeitüberwachung und Bilddatenspeicherung, dass über den Aufzeichnungszweck hinausgehende, gezielte Mitarbeiterkontrolle ausgeschlossen ist etc)
 - Ausnahmslose Kennzeichnungspflicht – Verbot verdeckter Videoüberwachung

- **Datenschutz-Technologien**, die KonsumentInnen selbst nutzen können (zur Verschlüsselung, Anonymisierung von Daten), müssen gefördert werden. **ZB Daten mit „Ablaufdatum“**: Verbraucher sollen Einträge im Internet mit einem Zeitstempel versehen können, die nach Zeitablauf alle automatisch gelöscht werden.

- Bei **neuen Anwendungen**, die potentiell in die Privatsphäre eingreifen (wie zum Beispiel RFID), muss vor deren Markteinsatz geklärt ist, wie die Privatsphäre geschützt und Missbrauch verhindert werden kann (zB Pflicht zur Datenschutz-Zertifizierung)

...für den öffentlichen Bereich

- Im öffentlichen Bereich sollten Planung, Ausschreibung und Umsetzung von Maßnahmen in Hinblick auf Datenschutzfolgen unabhängig bewertet werden: Privacy Impact Assessment (PIA) ist verpflichtend vorzuschreiben, die Nutzung von **Datenschutzertifizierungen** zu fördern (zum Beispiel dem Europäischen Datenschutzgütesiegel EuroPriSe).
- Die EU-Richtlinie über **Vorratsdatenspeicherung** sollte erst nach Prüfung grundrechtlicher Vorbehalte und nur in der schonendsten Form (kürzestmögliche Speicherung, Datenauskunft nur bei Terrorismusverdacht) umgesetzt werden.
- Rechtsstaatliche Grundsätze (Gewaltentrennung, unabhängige Kontrolle) sind strikt zu beachten. Besondere Bedeutung bei der Entscheidung, ob individuelle Rechte beschnitten werden dürfen, kommt der **richterlichen Kontrolle** zu.
- Kommt es zu Datenschutzverstößen oder Datensicherheitsproblemen müssen Datenschutzkommission und Betroffene von der verantwortlichen Behörde **informiert** werden.

... und ganz allgemein:

- **Datenschutz Gütezeichen:** vorbildliches Datenschutzverhalten muss sichtbar werden. Nicht jede Datensammlung kann von Datenschützern kontrolliert werden, deshalb braucht es Anreize, dass Datenverantwortliche Datenbanken, Software, Sicherheitssysteme etc. freiwillig testen lassen. Dafür gibt es ein Gütezeichen und einen öffentlichen Imagegewinn. Deutschland ist Vorreiter – Österreich sollte nicht hinterhinken.
- Die **Datenschutzbehörde** muss personell besser ausgestattet werden, um zB Ombudsmannfunktionen ausüben zu können. Ein eigenes Prüfzentrum für Datensicherheit, so wie in Deutschland, ist notwendig.

TIPPS der AK-Konsumentenschützer

- Erteilen Sie grundsätzlich keine Zustimmung zur Weitergabe Ihrer Daten. Gehen Sie mit Ihren Daten sorgsam und zurückhaltend um.
- Sehen Sie im Datenverarbeitungsregister nach, wer welche Daten über Sie gespeichert hat. Leider sind Standarddaten bei Massengeschäften nicht meldepflichtig.
- Wenn Sie eine schriftliche Auskunft über Ihre Daten verlangen, muss der Datenverwender Sie über Art, Herkunft, Empfänger, Zweck, eventuell beigezogene Dienstleister und die Rechtsgrundlage der Datenverarbeitung informieren.
- Untersagen Sie dem Datenverwender bei Bedarf (schriftlich) eine Weitergabe Ihrer Daten an andere Unternehmen.
- Für Beschwerden allgemein gegen Datenverwender des öffentlichen Bereichs (aber auch bei Beschwerden wegen Auskunftspflichtverstößen von privatwirtschaftlichen Datennutzern) ist die Datenschutzkommission im Bundeskanzleramt zuständig.
- Sie müssen nur für den Vertragsabschluss notwendige Daten weitergeben, darüber hinaus gehende Daten können Sie verweigern.
- Lesen Sie die Allgemeinen Geschäftsbedingungen von Verträgen und die Bestellformulare genau durch. Streichen Sie Klauseln wie "Ich bin mit der Weitergabe meiner Daten einverstanden".
- Haben Sie einer Datenverwendung zugestimmt, können Sie das jederzeit widerrufen. In anderen Fällen können Sie widerrufen, wenn Sie ein überwiegendes schutzwürdiges Geheimhaltungsinteresse haben.
- Vorformulierte Zustimmungserklärungen für die Datenweitergabe müssen verständlich sein. Wird zB nur auf die Weitergabe der Daten an Konzernunternehmen verwiesen, die sich jederzeit ändern können, ist das intransparent.
- Meiden Sie Gewinnspiele – sie dienen nur der Datensammlung.
- Lassen Sie sich auf Internetseiten als Benutzer registrieren, werden Ihre Daten gespeichert und oft weiter verwendet. Daher: Besorgen Sie sich eine zweite Gratis-E-Mailadresse und geben Sie eine falsche Anschrift bekannt. Das gilt natürlich nicht bei Vertragabschlüssen.
- Belästigen Sie unerwünschte Werbeanrufer so können Sie diesen Verstoß gegen Datenschutz- und Telekomregeln bei den Fernmeldebehörden anzeigen.