## Humanistische Union

# Mehr Datenschutz in der Wirtschaft ? Gewinn und Sicherheit für alle!

Aus: Mitteilungen Nr. 202, S. 3-6

Mehr Datenschutz in der Wirtschaft – Gewinn und Sicherheit für alle!

*Das Thema Datenschutz hat nach den jüngsten Skandalen plötzlich wieder Konjunktur. Viele, die in den letzten Jahren teils bedenkenlos, teils mit Bauchschmerzen alle möglichen Maßnahmen von biometrischen Merkmalen über Vorratsdatenspeicherungen bis hin zu Lauschangriffen und erweiterten Befugnissen für die Geheimdienste zugestimmt haben, entdecken nun wieder den Datenschutz. Das ist begrüßenswert, ob die Bemühungen jedoch glaubwürdig sein können, wird sich zeigen müssen. Noch ist vor allem von „drastischen Strafen", und „höheren Bußgeldern" die Rede, aber in der Substanz bleiben die Vorschläge dünn und kosmetisch – wie die aktuelle Datenschutznovelle etwa, bei der zu befürchten steht, dass sie den Datenschutz noch weiter aufweicht statt ihn zu stärken.*

#### Mehr Bedrohungen im privaten Bereich

Ein großer Discounter eröffnete den Reigen der Datenskandale und fiel durch eine Überwachung auf, die sich eigentlich gegen die eigenen Mitarbeiter richtete, um deren Arbeitsverhalten zu überwachen. Die Furcht vor Missbrauch von EC-Kundendaten wurde skandalisiert, die Tatsache der systematischen Überwachung von Mitarbeitern am Arbeitsplatz jedoch interessierte kaum jemanden. Niemand weiß wirklich, wie viele Orte und Betriebe etwa heute videoüberwacht sind. Da dies einen permanenten Eingriff in Arbeitnehmer- und Bürgerrechte bedeutet, sollten Videoüberwachungen in Unternehmen – vor allem im Kundenbereich – grundsätzlich deutlich gekennzeichnet sein und auf die zuständigen Aufsichtsbehörden hinweisen müssen, damit Bürger sich an diese wenden können und im Beschwerdefall die rechtmäßige Verwendung, Datensicherung und Löschung der Videodaten leichter überprüft werden kann.

#### Betriebliche Datenschutzbeauftragte müssen unabhängiger und qualifizierter werden

Leider wurde bei der letzten Datenschutznovelle die Schwelle für die Verpflichtung, einen betrieblichen Datenschutzbeauftragten zu berufen, auf zehn Mitarbeiter hoch gesetzt. Stattdessen müsste doch gefordert werden, diese Verpflichtung viel früher anzusetzen, denn die Rechenleistungen von Computern und die Kapazitäten von Speichermedien erlauben heutzutage, dass immer weniger Menschen immer größere Datenfluten bewältigen können und somit auch viel mehr Verantwortung tragen.

Entscheidend jedoch ist die Forderung, dass die Datenschützer in der Wirtschaft unabhängiger werden. Es ist kaum nachvollziehbar, dass das Datenschutzgesetz beispielsweise erlaubt, dass auch der stellvertretende

Geschäftsführer eines Unternehmens, das mit Daten handelt, sein eigener betrieblicher Datenschutzbeauftragter sein darf! So wird per Gesetz Vorschub geleistet, dass es einen wirkungsvollen Datenschutz in der Privatwirtschaft, vor allem der mittelständischen Wirtschaft, nur dort gibt, wo das Unternehmen sich ohnehin positiv zum Datenschutz bekennt.

Besonders für den Mittelstand sind unter Effizienzgesichtspunkten Lösungen interessanter, die wirkliche Fachkompetenz von außen heranholen und geprüften Dienstleistern die Funktion eines möglichst unabhängigen betrieblichen Datenschutzbeauftragten zu übertragen, statt dies durch unkundige Mitarbeiter als Alibi erledigen zu lassen. Selbst die als nicht datenschutzfreundlich geltenden USA gehen verstärkt diesen Weg. So schreibt die International Association of Privacy Professionals (IAPP) ihren zertifizierten Mitgliedern laufende Schulungen und wiederholte Zertifizierungen vor. Dieses System wäre vorbildlich, wenn dazu noch Datenschützer für die Wirtschaft – analog Anwälten, Steuerberatern oder vereidigten Wirtschaftsprüfern – nicht nur auf ihre Fachkunde hin geprüft, sondern auch strengen Zulassungsregeln hinsichtlich ihrer Berufsausübung unterworfen würden.

**...und in den Datenschutz investieren!**

Eine weitere wichtige Unterstützung für den Mittelstand wäre es, Datenschutzaudits in kleinen oder mittleren Unternehmen (KMU) aus EU-Mitteln zu fördern. Denn um KMU für den Datenschutz fit zu machen, fehlt es im Alltag oft nicht an der Bereitschaft, sondern am zusätzlichen Kleingeld für das entsprechende Know-how. Was könnte neben der Förderung ein Anreiz für die Wirtschaft sein, mehr für den Datenschutz zu tun? Neben den Vorteilen von Datenschutzaudits und von Zertifizierungen sollte der Gesetzgeber die private Datenhaltung transparent machen.

**Risiken dort bekämpfen, wo sie entstehen**

Sicherlich wäre es nicht angemessen, Unternehmen, die mit sensiblen Personendaten umgehen und umgehen müssen, grundsätzlich Ignoranz oder Bereitschaft zur Illegalität zu unterstellen. Das Verhältnis von Konzernsicherheit und Datenschutz in der Wirtschaft ist wohl ähnlich gestaltet, wie beim Staat jenes zwischen den Geheimdiensten und den Datenschützern. Letztere werden eher als lästige Aufpasser empfunden und wenn überhaupt, dann regelmäßig im Nachhinein und restriktiv über Operationen in der Grauzone informiert. Um so vordringlicher ist es, die Stellung der betrieblichen Datenschutzbeauftragten auch in Großunternehmen, wo sie hauptamtlich beschäftigt sind, zu stärken, damit sie ohne Einschränkung direkt an den Vorstand berichten und sich auch selbst an die Aufsichtsbehörden oder die Öffentlichkeit wenden können, wenn sie Verstöße feststellen und keine Abhilfe erfolgt. Darüber hinaus ist zu fordern, dass sie auch mit einem eigenen Budgetrecht auszustatten sind, das ihnen erlaubt, von ihnen als kritisch erkannte Prozesse durch unabhängige Sachverständige auditieren zu lassen.

**Prinzip der Datensparsamkeit auch in der Privatwirtschaft durchsetzen!**

Das Prinzip der Datensparsamkeit, ein Grundsatz, den das Bundesverfassungsgericht 1983 formuliert hat, sollte durch die folgenden drei Maßnahmen auch hinsichtlich der Wirkung auf die Wirtschaft wirksam

gestärkt werden:

1. Mit der gesetzlichen Festlegung der Datenerhebung nur nach ausdrücklicher Zustimmung des Betroffenen, die an keinerlei Vertragsbedingungen gekoppelt werden darf, als freiwilliger, positiver Akt – so genannte „Opt-in" Lösung. Diese muss für Preisausschreiben ebenso gelten, wie für jegliche Weiterverwendung von Geschäftsdaten etwa bei Telefonverträgen oder Rabattkarten.
2. Eine Ausgestaltung des Melderechts bundesweit dergestalt, dass es zur Weitergabe der Stammdaten außerhalb des öffentlichen oder gesetzlich geregelten Bereichs grundsätzlich der aktiven Zustimmung bedarf und ein jederzeitiges Widerspruchsrecht besteht, wie es das NRW-Meldegesetz von 1998 bis 2005 bereits einmal vorsah.
3. Mit einer Verpflichtung der Privatwirtschaft, dem erfassten Bürger einmal jährlich obligatorisch einen Datenkontoauszug zuzusenden, die im Bundesdatenschutzgesetz einheitlich geregelt werden sollte. Für die Telekommunikationswirtschaft, Banken, Versicherungen ebenso wie für viele andere Dienstleister wäre es einfach und nicht einmal ein nennenswerter Kostenfaktor, solche Datenkontoauszüge etwa mit der Monatsrechnung oder dem Kontoauszug zu versenden. Es würde aber manchem die Augen öffnen, wer alles wie viel über ihn oder sie weiß.

#### Aufsichtsbehörden sind unzureichend ausgestattet

Die wenigen positiven Beispiele aus der Wirtschaft können aber keine wirkungsvollen Gesetze ersetzen, denn diese sollen ja vor allem im Fall des Missbrauchs Wirkung entfalten. Deshalb bedarf es dringend der Stärkung der Kontrollbehörden über den privaten Bereich. Viel zu vage sind die Vorschriften, viel zu selten die Kontrollen und viel zu rudimentär ausgestattet die Aufsichtsbehörden, um Beschwerden wirkungsvoll nachgehen zu können. So sind im Baden-Württembergischen Innenministerium, der Behörde, die in ganz Südwestdeutschland für Verstöße im privaten Datenschutz zuständig ist, gerade einmal vier Mitarbeiter mit der Erfüllung dieser Aufgabe betraut, natürlich nur neben ihren anderen Aufgaben im Innenministerium. Das Regierungspräsidium Darmstadt dagegen verfügt für die gleiche Aufgabe über dreizehn Stellen. Der nordrhein-westfälischen Datenschutzbeauftragten, zuständig auch für den privaten Datenschutz und Informationsfreiheit, hat die Politik seit 2005 jährlich eine Stelle aus Haushaltsgründen gestrichen. Es ist überfällig, die Aufsichtsbehörden angesichts der explodierenden Datenströme im privaten Bereich stattdessen mit deutlich mehr Personal auszustatten, damit sie ihre gesetzlichen Aufgaben überhaupt erfüllen können.

#### Datenschutzkompetenz gehört zukünftig zur beruflichen Grundbildung

Vielen Menschen ist überhaupt nicht bewusst, wer aus der Privatwirtschaft bei welcher Gelegenheit Daten erfasst. Gerne spielen etwa autobegeisterte Bürger am Wochenende mit den „Konfiguratoren" der Hersteller und stellen sich zum Spaß ihren Lieblings-Porsche, Mercedes oder Audi zusammen. Dass über die Speicherfunktionen für persönliche Konfigurationen auch irgendwann einmal nach der E-Mail oder gar Personendaten wie Name und Adresse gefragt wird, fällt manchem gar nicht auf, oder erst dann, wenn er sich wundert, dass er plötzlich eine Werbeofferte bekommt, die ziemlich genau seinem Geschmacksprofil entspricht. Vieles, was inzwischen Softwareprogramme wie etwa Google-Analytics ermöglichen, um Konsumentenprofile zu erstellen, ist ohne Zustimmung der Betroffenen rechtswidrig.

Angesichts einer zunehmenden Menge sensibler, personenbezogener Daten auf Festplatten der Unternehmen und in privaten Speichern – von der Bank über die Krankenkasse bis zu Versicherungen, Internet-Providern, Telekommunikationsunternehmen und Payback-Datenverarbeitern – muss auf den Prüfstand, ob die dort beschäftigten Mitarbeiter in Datenschutzfragen hinreichend kompetent und genügend geschult sind, um sich

im Zweifelsfall illegalen Anweisungen ihrer Vorgesetzten zu widersetzen und diese ggf. auch anzuzeigen. In der Regel wird diese Frage zu verneinen sein. Deshalb besteht auch hier ein dringender Handlungsbedarf, um Datenschutzrisiken dort zu mindern, wo sie entstehen und besondere Sorgfalt im Umgang mit Daten geboten ist.

So ist zu fordern, dass Mitarbeiter und Mitarbeiterinnen, die mit personenbezogenen Daten umgehen, eine Mindestqualifikation erfüllen und diese durch ein Zertifikat nachweisen müssen. Es ist heute üblich, reicht im Informationszeitalter aber nicht mehr aus, Mitarbeiter per einfacher Erklärung, bei der meistens das „Kleingedruckte" gar nicht gelesen wird, auf das Datengeheimnis zu verpflichten.

Der Gesetzgeber könnte stattdessen vorschreiben, dass Zertifikate und andere Sachkundenachweise unabdingbare Voraussetzung sind, um etwa im Call-Center zu arbeiten und weitere Qualifikationen, um solche zu betreiben, denn gerade hier ist eine Gefahrenquelle für den Datenschutz aus der Sache heraus gegeben. Schließlich darf aus gutem Grund auch nicht, wer einen PKW-Führerschein besitzt, einen LKW mit Gefahrgütern führen.

Was für Call-Center gilt, betrifft natürlich in erheblichem Maße auch alle Branchen der Gesundheitswirtschaft, die durch die zunehmende Digitalisierung mit immer größeren Datenmengen operieren. Angefangen von den Mitarbeitern der kassenärztlichen Vereinigungen, die den zentralen Datenpool der Digitalen Gesundheitskarte verwalten, über die Angestellten der Krankenkassen bis hin zu medizinischen Zentren und Arztpraxen.

#### Was müssen Mitarbeiter mindestens über Datenschutz wissen?

Ein Modellprojekt für ein solches Datenschutz- und Datensicherheitszertifikat wird derzeit von den Landesmedienanstalten NRW und Rheinland-Pfalz unterstützt. Unterhalb des Fachkundenachweises, den betriebliche Datenschutzbeauftragte erbringen müssen, entsteht derzeit als Kooperation von „Klicksafe" Rheinland-Pfalz und der Dienstleistungsgesellschaft für Informatik in Bonn ein Zertifikat für Datenschutz und Datensicherheit für Schüler und darüber hinaus in Zusammenarbeit mit der Gesellschaft für Informatik ein solches für Mitarbeiter in der Wirtschaft.

Eine Verbesserung der Aus- und Weiterbildung von Mitarbeitern in Fragen des Datenschutz und der Datensicherheit ist bisher in vielen Bereichen der Wirtschaft vernachlässigt worden. Was können nun die Mindestanforderungen an Mitarbeiter sein, die „Skills" eines Datenschutz- und Datensicherheitszertifikats?

1. Neben Grundbegriffen der Datenverarbeitung und Sicherheitsfragen gängiger Software vor allem der Grundrechtscharakter des informationellen Selbstbestimmungsrechts. Dazu gehört der Grundsatz, dass personenbezogene Daten nur zweckgebunden, aufgrund eines Gesetzes oder aufgrund von freiwilliger Zustimmung genutzt, gespeichert, verarbeitet oder weitergegeben werden dürfen.
2. Das Wissen, dass eine Weitergabe nicht ohne Zustimmung der Betroffenen erfolgen sollte und dass Betroffene einen Auskunftsanspruch haben, woher ein Unternehmen ihre Daten hat und dass auf unbefugte Datennutzung und -weitergabe hohe Bußgelder und Strafen erhoben werden können.
3. Die Pflicht, solche Daten zu sichern und sie nicht mit anderen zu verknüpfen. Daraus folgen Sorgfaltspflichten im Umgang mit Daten und über die Dokumentation, wofür sie von wem genutzt oder abgerufen werden. Dies sind nur einige Beispiele, die Eingang in entsprechende Lernzielkataloge und Zertifizierungen finden sollten.
4. Einen Blick dafür, zu erkennen und sich zu informieren, welche Art von Prozessen, Geschäftspraktiken oder Techniken Risiken für Datenschutz und IT-Sicherheit mit sich bringen

könnten, um im Zweifelsfall den fachkundigen Rat von Datenschutz- oder IT-Fachpersonal in Anspruch zu nehmen.

**Neue Herausforderungen durch das Web**

Selbstverständlich kommen in Zeiten des Web 2.0 noch andere Dimensionen hinzu, die etwa die Verletzung von Persönlichkeitsrechten durch die Veröffentlichung vertraulicher Informationen im Netz oder auch nur die Weitergabe solcher Informationen, die nicht einfach wieder zurückgeholt oder gelöscht werden können. Viele Beispiele, etwa das Einstellen eines Videos über die letzte Party auf You-Tube, sind prinzipiell heute schon ahndungsfähige Verstöße gegen die Persönlichkeitsrechte der Betroffenen. Die Brisanz, neue rechtliche Instrumentarien zum Schutz der Persönlichkeit zu schaffen, bewies erst kürzlich der Launch des Portals www.rottenneighbour.com.

Es ist bislang nicht einfach, solche elektronischen Übergriffe gerichtlich zu verfolgen. Dem muss eine zukünftige Datenschutzgesetzgebung Rechnung tragen, etwa durch neue Verfahren, Schadenersatzansprüche aus verletztem Persönlichkeitsrecht geltend machen zu können. So sollten Privatpersonen, deren Daten ohne Zustimmung von dritten ins Netz gestellt werden, den Verursacher auch zivilrechtlich verfolgen können. Die Probleme der Identifikation sollen dabei natürlich nicht unterschlagen werden. Es gibt geeignete Methoden, die es ermöglichen, z. B. die IP-Adresse unkenntlich zu machen, was an sich nicht verwerflich, sondern in bestimmten Fällen sogar von Datenschützern empfohlen wird. Gleichwohl müssen wir über international wirksame Rechtsverfolgung auch im Privatrecht nachdenken, die auch gegen Provider oder Akteure im Ausland wirksam ist, die neu erdacht und entwickelt werden muss, um bei der Verletzung von Persönlichkeitsrechten im Netz und aus dem Netz nicht nur die Beseitigung verlangen zu können, sondern die auch wirksam Schadenersatz durchzusetzen vermag.

**Neue Herausforderungen durch digitalen Geschäftsverkehr und E-Commerce**

Zahlreiche Betrugsfälle der Vergangenheit, nicht zuletzt im Zusammenhang mit diversen Internetplattformen, aber auch im elektronischen Banken- und Geschäftsverkehr, könnten durch Zertifizierungen verhindert werden. Leider fehlt in Deutschland immer noch ein Auditgesetz, das den gesetzlichen Rahmen und die Mindestanforderungen für Zertifikate formuliert. Bisher gilt nur eine entsprechende Regelung in Schleswig-Holstein, in Zeiten des grenzüberschreitenden europäischen Binnenhandels auch im elektronischen Handel ein schlichter Anachronismus. Deshalb muss ein Datenschutz-Auditgesetz, das auch die Kreditratings einschließt, wie sie heute von Banken, Agenturen und Auskunfteien angeboten werden, Klarheit und mehr Verbraucherschutz schaffen.

Ein positives Beispiel für erfolgreiche Regelungen in Selbstorganisation der Wirtschaft bieten die unter dem Dach der Initiative D21 e.V. organisierten Gütesiegel im Internet. Diese haben sich freiwillig auf hohe Standards des Verbraucher- und Datenschutzes verpflichtet und unterwerfen sich der Kontrolle eines Gütesiegelboards, dem neben den Gütesiegelunternehmen unabhängige Experten und Vertreter von Datenschutzbeauftragten und Verbraucherschutzorganisationen angehören. Die positiven Beispiele aus der Wirtschaft müssen durch praktikable Gesetze zur Regel werden. Und auch da gibt es auf mehreren Feldern dringenden Handlungsbedarf.

Die seit 2005 in verschiedenen Schritten beschlossenen Wege zur Einführung der digitalen Signatur bedeuten ebenfalls neue Herausforderungen für Datenschutz und insbesondere die Datensicherheit im privaten Bereich. Noch sind für Verbraucher die Risiken ihrer elektronischen Zahlungsmittel bei aller technischen Unzulänglichkeit der EC-Karten oder Kreditkarten mit PIN überschaubar. Ob dies noch der Fall

sein wird, wenn künftig die digitale Signatur nicht nur auf der Sparkassenkarte, sondern auch auf dem Personalausweis, der Gesundheitskarte und ELENA, dem elektronischen Gehaltsnachweis enthalten sein wird, wird sich zeigen. Ob die mit der Signatur einher gehende Beweislast-Umkehr zu Lasten der Verbraucher ein Schritt zu mehr Verbrauchersicherheit war, ist in diesem Zusammenhang zu bezweifeln und sollte deshalb schnell überprüft werden.

**Zertifizierung für Unternehmen klar regeln**

Viele Beispiele in der Privatwirtschaft zeigen schon heute hohes Verantwortungsbewusstsein der Verantwortlichen. Von Trust-Centern, die unter strengsten Kriterien zertifiziert werden, aber auch von Banken, die aufgrund interner und versicherungsrechtlicher Absicherungen dazu angehalten sind, werden überaus hohe Standards erreicht. Von der europäischen Sicherheits- und Datenschutznorm ISO 17799 über Datenschutz-Gütesiegel, wie sie etwa das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein vergibt, bis zu den unter dem Dach der Initiative D21 organisierten Gütesiegeln gilt für unterschiedliche Anwendungsbereiche der Wirtschaft eine große Spannweite von Kriterien des Datenschutzes, der Datensicherheit und des Verbraucherschutzes, die jedoch praktisch nur wenigen Fachleuten bekannt sind. Diese Kriterien müssen transparent und vor allem den Verbrauchern näher gebracht werden, auch darin läge die Aufgabe eines vernünftigen Auditierungsrahmens. Denn wie in vielen Bereichen sind auch hier inzwischen Fälscher und Manipulierer unterwegs, auch hier gilt es sich abzugrenzen gegen wertlose Siegel, wie sie heute schon im Internet kursieren.

Leider stehen einige Politiker einem wirksamen Auditgesetz immer noch skeptisch gegenüber. Der vorliegende Entwurf wird den Anforderungen an einen wirksamen Datenschutz unter den Bedingungen moderner Datenverarbeitung nur unzureichend gerecht. Gleichwohl findet insofern eine "Abstimmung mit den Füßen" statt, als immer mehr Unternehmen von sich aus nach Zertifizierungen rufen. So verzeichnen Unternehmen wie der TÜV Süd Management GmbH eine gestiegene Nachfrage nach Zertifizierungen und können sich Unternehmen wie Datenschutz Nord GmbH, einst eine Strukturinitiative für Bremerhaven, inzwischen erfolgreich als bundesweit tätige Unternehmen etablieren. Auch die anderen Gütesiegel unter dem Dach der Initiative D21 verzeichnen deutliche Zuwächse. Der Politik kommt die Entscheidung zu, wirksame Gütesiegel von Placebos zu unterscheiden. Datenschutz ist wie Umweltschutz längst kein lästiges Kostenelement mehr, sondern schafft Arbeitsplätze und wird durch das Vertrauen der Verbraucher zum positiven Faktor in der Wertschöpfungskette.

**Neue politische Signale notwendig**

Die Auswüchse des vermeintlichen „Kampfes gegen den Terror" haben in den letzten Jahren gehörig mit zur Aushöhlung des Datenschutzbewusstseins beigetragen, indem gegen den Rat von Bürgerrechtlern und Datenschützern immer neue Datenerfassungen, von der Rasterfahndung über biometrische Daten, die einheitliche Steuernummer bis zur Vorratsdatenspeicherung von Telefonverbindungen fast alles Denkbare auch beschlossen wurde. Insofern muss mancher Datenskandal dieser Tage das Rechtsbewusstsein aller sensibilisieren. Es sollte zu denken geben, wenn es in immer kürzeren zeitlichen Abständen dem Bundesverfassungsgericht vorbehalten ist, die Wellen der Überwachungsgesetze zu stoppen, und die Tatsache an sich lässt befürchten, dass es um das Verhältnis der politischen Mehrheiten zu den Grund- und Freiheitsgarantien des Grundgesetzes schlecht bestellt ist.

**Ein Grundrecht auf Datenschutz ins Grundgesetz**

Am 19. Dezember 1978 wurde das Grundrecht auf Datenschutz in die Verfassung Nordrhein-Westfalens aufgenommen. Seitdem herrschen Stillstand und Rückschritt beim Gesetzgeber um ein elementares Bürgerrecht, das wie kein anderes erst durch die informationstechnische Entwicklung an Bedeutung gewonnen hat. Eine breite politische Diskussion, ob ein Individualrecht auf Datenschutz im Grundgesetz zusätzlich formuliert werden sollte, ist überfällig und darf nicht weiter den Gerichten überlassen werden. Ein verbrieftes individuelles Grundrecht auf Datenschutz und die Informationsfreiheit gegenüber dem demokratischen Staat sind zwei Seiten einer Medaille. 60 Jahre nach Verabschiedung des Grundgesetzes würde unserer Demokratie die Kodifizierung des Datenschutzes und der Informationsfreiheit gut anstehen, zumal andere westliche Demokratien wie Schweden, Norwegen, Kanada und Frankreich längst über vergleichbare Rechtsordnungen verfügen. Es besteht insbesondere deshalb eine Chance, weil ein solcher Verfassungsvorschlag nicht hinter das Informationelle Selbstbestimmungsrecht zurückfallen kann, dass das Bundesverfassungsgericht direkt aus Artikel 1 Grundgesetz und aus dem Demokratieprinzip abgeleitet hat und damit einer „Ewigkeitsgarantie" unterliegt. Eine klare Formulierung könnte das Bewusstsein für eine freiheitliche Verfassungswirklichkeit stärken und manchem Drang zur schleichenden Aushöhlung elementarer Grundrechte Einhalt gebieten.

„*Time for a Change*" im Datenschutz: Es an der Zeit, sich auch von Seiten der Wirtschaft eindeutig auf die Seite einer offenen Gesellschaft und der Bürgerrechte zu stellen und es gibt viele Möglichkeiten für Unternehmen, hierfür eigene freiwillige Beiträge zu leisten!

*Roland Appel*
*ist Politikwissenschaftler und Unternehmensberater ,*
*Vorsitzender des Gütesiegelboards der Initiative D21 e.V. und*
*Mitglied der G-10 Kommission des Landtages Nordrhein-Westfalen*

---

https://www.humanistische-union.de/publikationen/mitteilungen/202/publikation/mehr-datenschutz-in-der-wirtschaft-gewinn-und-sicherheit-fuer-alle/
Abgerufen am: 10.11.2026