

Datenschutz newsbox



Ausgabe

2

2/2012

- Mentana-Claimsoft erhält Datenschutz-Zertifikat für De-Mail-Lösung 3
- DGRI fordert weitere Revision des Datenschutzrechts auf EU-Ebene 3
- BSI veröffentlicht Empfehlungen für sicheren PC-Betrieb 4
- BfDI zur Modernisierung des Datenschutzes 4
- Betriebsrat darf Protokolldaten nicht grundlos einsehen 5
- Private Nutzung eines Diensthandys rechtfertigt fristlose Kündigung 5
- Europäischer Datenschutz-Dachverband zur EU-Datenschutzverordnung: „Datenschutzbeauftragte – Europäische Hüter der Privatsphäre“ 6
- Schuldnerverzeichnis im Internet: Datenschützer kritisieren elektronisches Schuldnerverzeichnis 6
- Aus der Welt des Tracking und des Online Behavioural Advertising 7
- GDD**-Fachtagung:
Die neue EU-Verordnung zum Datenschutz 7



Editorial:

Was haben Facebook und das Jobcenter Pankow gemeinsam?

Die erste Gemeinsamkeit ist sicherlich, dass sowohl Facebook als auch das Pankower Jobcenter von einer großen Zahl von Menschen personenbezogene Daten besitzen. Der Unterschied ist, dass die Benutzer von Facebook den Datenstriptease aus freien Stücken aufs Parkett legen. Im Gegensatz zu den Facebook-Usern bleibt den Kunden der Jobcenter/des Jobcenters meist keine andere Alternative als ihre personenbezogenen Daten zu offenbaren, wenn sie in den Genuss der benötigten Unterstützung kommen möchten.

Eine weitere Gemeinsamkeit scheint die beiden jedoch auch noch zu einen. Der Umgang mit Löschfristen, wenn es um personenbezogene Daten geht.

§ 84 Abs. 2 SGB X fordert:

„Sozialdaten sind zu löschen, wenn ihre Speicherung unzulässig ist. Sie sind auch zu löschen, wenn ihre Kenntnis für die verantwortliche Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden.“

Umso verwunderlicher ist es, dass die zumindest bei dem Jobcenter Pankow genutzte Software anscheinend eine Löschung in technischer Hinsicht gar nicht vorsieht.

Eine ähnlich entspannte Vorgehensweise legt die Firma Facebook an den Tag, wenn es um die Löschung personenbezogener Daten, genauer, wenn es um die Löschung von eingestellten Fotos geht. Einem Bericht des Technik-Blogs Ars Technica zu Folge hält Facebook Bilder auch mehrere Jahre, nachdem die Facebook-User diese gelöscht haben, auf seinen Server vor. Ein Abruf ist nach der vom User angestoßenen Löschung auch drei Jahre danach möglich, wenn Dritte nur den direkten Link auf die Bild-URL kennen.

Es gibt aber auch noch einen großen Unterschied zwischen den beiden Sachverhalten, zumindest in der Wahrnehmung durch Nicht-Betroffene. Das Gebaren von Facebook löst bei so manchem eine große Empörung aus. Zumindest mehr als über das Gebaren des Job-Centers.

Ihr
RA Levent Ferik

Mentana-Claimsoft erhält Datenschutz-Zertifikat für De-Mail-Lösung

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar hat der Mentana Claimsoft GmbH ein Datenschutzzertifikat für den dort geplanten De-Mail-Dienst erteilt. Darin wird bestätigt, dass die Mentana Claimsoft GmbH die datenschutzrechtlichen Anforderungen des De-Mail-Gesetzes erfüllt.

Die Erteilung der Bescheinigung ist Bestandteil des Akkreditierungsverfahrens beim BSI, das jeder Anbieter von De-Mail-Diensten im Vorfeld durchlaufen muss.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist gemäß De-Mail-Gesetz zuständig für die Erteilung des Zertifikates, das die Datenschutzkonformität der geplanten De-Mail-Dienste bestätigt. Dabei prüft er die Einhaltung der datenschutzrechtlichen Anforderungen anhand eines Gutachtens einer anerkannten oder öffentlich bestellten oder beliebigen

sachverständigen Stelle für den Datenschutz. Der Gutachter wiederum hat bei seiner Prüfung die Anforderungen zu beachten, die in einem Kriterienkatalog festgelegt sind. Der De-Mail-Kriterienkatalog für den Datenschutznachweis ist auf der Website des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unter <http://www.bfdi.bund.de/DE/Schwerpunkte/DE-Mail/InformationenAnbieter/Artikel/KriterienkatalogNachweis.html?nn=1958446> veröffentlicht.

Das Angebot von De-Mail-Diensten ist ein von der Bundesregierung gefördertes Projekt zum sicheren und verbindlichen Austausch von elektronischen Dokumenten mittels E-Mail. Kernbestandteil des De-Mail-Dienstes ist der Postfach- und Versanddienst, welcher eine zuverlässige und vertrauliche Kommunikation, sowie den gleichermaßen geschützten Versand von Dokumenten mittels E-Mail ermöglicht.

Quelle: Pressemitteilung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

DGRI fordert weitere Revision des Datenschutzrechts auf EU-Ebene

Die Initiative der EU für einheitliche Datenschutzstandards in Europa hat in Deutschland ein grundsätzlich positives Echo gefunden. Zu den Details wurde aber auch deutliche Kritik laut, u. a. auch von der Deutschen Gesellschaft für Recht und Informatik e.V. (DGRI).

Die Deutsche Gesellschaft für Recht und Informatik e.V., eine der in Deutschland führenden unabhängigen wissenschaftlichen Vereinigungen im Bereich des IT-Rechts; zu ihren Mitgliedern zählen Richter, Rechtsanwälte, Rechtswissenschaftler, Firmenjuristen der IT-Branche und IT-Techniker, hat sich ebenfalls mit einer kritischen Stellungnahme zum Entwurf der geplanten EU-Datenschutzverordnung zu Wort gemeldet. Die DGRI e.V. befasst sich mit Fragen im Bereich der Schnittstelle zwischen Informatik- und EDV-Recht einerseits sowie Recht und Wirtschaft andererseits.

Die DGRI stellt klar, dass sie das Bestreben der Kommission, das national sehr unterschiedliche Datenschutzrecht durch eine Verordnung europaweit zu vereinheitlichen und dadurch Unsicherheiten über die jeweils anwendbaren Regelungen erheblich zu reduzieren begrüßt und regt jedoch gleichzeitig an, bei der Neugestaltung des Datenschutzes in Europa die Gelegenheit zu nutzen, um das Schutzkonzept einer Revision zu unterziehen. Dabei seien nachfolgende Grundsätze zu beachten, um so dem Datenschutz zu größerer Akzeptanz und Effektivität zu verhelfen. Zur Untermauerung des Revisionsbedürfnisses stellt die DGRI 9 Grundsätze vor, wie z. B. die Tatsache, dass das geltende Datenschutzrecht tiefgehende Differenzierung des Begriffs der personenbezogenen Daten durchführt. Einer fast binären Denkweise unterworfen, sind personenbezogene Daten entweder personenbezogen und unterfallen damit dem strengen Regime des Datenschutzrechts oder es handelt sich eben nicht um personenbezogene Daten.

Die detaillierten Ausführungen zu den restlichen ausgearbeiteten Grundsätzen lassen sich unter dem nachfolgenden Link nachlesen.

Quelle: Pressemitteilung der Deutsche Gesellschaft für Recht und Informatik e.V.

BSI veröffentlicht Empfehlungen für sicheren PC-Betrieb

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Empfehlungen für den sicheren Betrieb von Windows-PCs zusammengestellt und anlässlich des europaweiten „Safer Internet Day“ am 7. Februar 2012 Empfehlungen zur sicheren Konfiguration von Windows-PCs veröffentlicht.

Die BSI-Empfehlungen bieten Anwendern konkrete Hilfestellungen bei der sicheren Konfiguration eines Windows-PCs für die private Nutzung sowie in einer zweiten Version für die Nutzung in kleinen Unternehmen. Dabei wird der komplette Lebenszyklus eines PCs vom Kauf des Systems über die Installation und Inbetriebnahme, den regelmäßigen Betrieb bis hin zur Entsorgung betrachtet. Mithilfe der BSI-Empfehlungen können die Nutzer ihre Rechner unter einem aktuellen Microsoft Windows so einrichten, dass eine weitgehend sichere Nutzung von Dienstleistungen über das Internet möglich ist.

Im Rahmen der neuen Reihe „BSI-Empfehlungen zur Cyber-Sicherheit“ veröffentlicht das BSI daher in der Rubrik „Produktkonfiguration“ Empfehlungen zur sicheren Konfiguration von ausgesuchten, gängigen IT-Produkten und -Anwendungen. Dabei geht es nicht um die Darstellung einer hundertprozentigen theoretischen Sicherheit, sondern vielmehr darum, in der Praxis die größtmögliche Sicherheit bei vertretbarem Aufwand zu erreichen.

Vielleicht für einige überraschend empfiehlt das BSI als sichere Browser-Alternative Google Chrome. Ausschlaggebender Grund dafür sei die Sandbox-Funktion und die Auto-Update-Funktion, die die Sicherheit deutlich erhöhen, erklärt der Leitfaden. Zu einem ähnlich positiven Ergebnis bzgl. der Sicherheit bei der Benutzung des Browsers aus dem Hause Google war bereits Ende 2011 eine andere Studie gekommen.

Quelle: Bundesamt für Sicherheit in der Informationstechnik

BfDI zur Modernisierung des Datenschutzes

Die Vorschläge der Europäischen Kommission für einen neuen Datenschutz-Rechtsrahmen stellen nach Auffassung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit Peter Schaar eine gute Grundlage dar, auf deren Basis allerdings noch einige Verbesserungen vorgenommen werden sollten. Das Datenschutz-Paket biete die Chance für einen europaweit wirksameren Schutz personenbezogener Daten. Schaar erwarte von der Bundesregierung, dass sie sich in den anstehenden Beratungen auf EU-Ebene aktiv für einen verbesserten Datenschutz einsetzt. Dies gelte insbesondere für den Datenschutz im Verhältnis zu Nicht-EU-Staaten.

Angesichts der zunehmenden Bedeutung des Internets begrüße Schaar, dass die strengen Grundsätze des EU-Rechts generell auch dann gelten sollen, wenn sich Unternehmen aus Nicht-EU-Ländern mit ihren Diensten an Bürger in der EU wenden, selbst wenn sie keine Niederlassung in Europa haben.

Ebenfalls positiv wird vom BfDI die Verpflichtung zur Verwendung datenschutzfreundlicher Technologien („Privacy by Design“) und Grundeinstellungen („Privacy by Default“) bewertet. Für soziale Netzwerke bedeute dies etwa, dass die Daten der Nutzer nicht von vornherein der Öffentlichkeit zugänglich gemacht werden dürfen, sondern nur nach ausdrücklicher Freigabe durch den Nutzer.

Angesichts der guten Erfahrungen in Deutschland begrüße Schaar, dass die Kommission die Bestellung der betrieblichen und behördlichen Datenschutzbeauftragten europaweit verbindlich machen will.

Nach geltender Rechtslage muss ein Unternehmen bereits dann einen Datenschutzbeauftragten bestellen, wenn zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt werden. Nach der VO kann die Bestellung zudem auf zwei Jahre begrenzt werden. Der Bundesbeauftragte sieht aber auch eine Schwächung des Prinzips der betrieblichen Selbstkontrolle durch die in Art. 35 des Entwurfs der Verordnung geregelte grundsätzliche Bestellpflicht für einen betrieblichen Datenschutzbeauftragten bei einer Unternehmensgröße von mehr als 250 Mitarbeitern. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit geht davon aus, dass nur noch 0,3 Prozent der deutschen Unternehmen zur Bestellung eines Datenschutzbeauftragten verpflichtet würden. Er tritt damit für eine deutlich niedrigere Grenze ein.

Quelle: Pressemitteilung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Betriebsrat darf Protokolldaten nicht grundlos einsehen

Das Arbeitsgericht Wesel hat in einem Beschluss vom 17.11.2011 (Az.: 5 BV 17/11) einen Anspruch eines Betriebsrats gegen den Arbeitgeber auf eine umfassende Einsichtnahme in die Protokolldateien für Zugriffe auf das Betriebsratslaufwerk verneint. Nach Auffassung des Arbeitsgerichts Wesel fehlt ein dafür erforderliches Rechtsschutzbedürfnis des Betriebsrates selbst bei zuvor erfolgter unbefugter Einsichtnahme in Betriebsratsdateien durch den Arbeitgeber.

Der Arbeitgeber hatte eingeräumt, dass er in einem Fall Zugriff auf die Datenhistorie einer Datei des Betriebsrats genommen hatte. Zuvor war ihm der Inhalt der Datei selbst vom Betriebsrat zugänglich gemacht worden. Daraufhin hatte das Arbeitsgericht We-

sel in einem Vorverfahren bereits den Arbeitgeber aufgefordert, dieses zukünftig zu unterlassen. Nun wollte der Betriebsrat Einsicht in die Protokolldateien für Zugriffe auf das Betriebsratslaufwerk nehmen. Dieses Recht machte er vor Gericht geltend.

Der Arbeitgeber lehnte das ab und begründete das unter anderem mit dem Datenschutz: Bei einer Auswertung müssten auch personenbezogene Daten von zahlreichen Mitarbeitern eingesehen werden. Außerdem warf er dem Betriebsrat vor, jetzt selbst spionieren zu wollen: Es gehe ihm nicht mehr darum, die eigenen Daten zu schützen, das Ziel sei «allein die Ausforschung» des Arbeitgebers.

Zu den Details der Entscheidung siehe unten folgende Quellenangabe.

Quelle: Justiz.NRW

Private Nutzung eines Diensthandys rechtfertigt fristlose Kündigung

Wer sein Diensthandy für private Gespräche nutzt, obwohl diese vom Arbeitgeber nicht gestattet wurden, kann fristlos gekündigt werden. Eine vorherige Abmahnung ist dabei nicht zwingend erforderlich. Dies geht aus einer Entscheidung des Landesarbeitsgerichts Hessen hervor.

Der Entscheidung lag die Klage eines Hubwagenfahrers gegen die Lufthansa-Service-Gesellschaft (LSG) zu Grunde (Urt. 25.07.2011, Az. 17 Sa 153/11). Der Kläger war mehr als 25 Jahre bei der LSG beschäftigt.

Nach dem der Arbeitgeber nach der Rückkehr des Arbeitnehmers aus dem Urlaub vom Netzbetreiber des genutzten Diensthandys eine Rechnung über Auslandsgespräche in Höhe von mehr als 500 EUR erhielt, sprach er dem Arbeitgeber die fristlose Kündigung aus. Das Arbeitsgericht Frankfurt, welches in erster Instanz für den Fall zuständig war, kam zu dem Ergebnis, dass die fristlose Kündigung mangels einer vorherigen Abmahnung unzulässig sei.

Die 17. Kammer des Hessischen Landesarbeitsgerichts bewertete den Sachverhalt jedoch anders und entschied, dass eine ausgiebige Privatnutzung eines Diensthandys auf Kosten des Arbeitgebers stets ein Grund für eine fristlose Kündigung sei und damit auch keiner vorherigen Abmahnung bedürfe. Dem Arbeitnehmer hätte auch ohne einen Hinweis diesbezüglich klar sein müssen, dass der Arbeitgeber Privatgespräche nicht in einem Umfang von mehreren hundert Euro akzeptieren werde. Daran ändere auch seine 25-jährige Betriebszugehörigkeit nichts.

Quelle: Hessenrecht Landesrechtsprechungsdatenbank

Europäischer Datenschutz-Dachverband zur EU-Datenschutzverordnung: „Datenschutzbeauftragte – Europäische Hüter der Privatsphäre“

Die Europäische Kommission hat am 25. Januar 2012 den Entwurf einer neuen EU-Verordnung beschlossen, die den Schutz der Privatsphäre in der EU zukunftsfähig gestalten soll.

Die „Confederation of European Data Protection Organisations (CEDPO)“ hat die in dem EU-Verordnungsentwurf angelegte Schlüsselrolle der betrieblichen und behördlichen Datenschutzbeauftragten bei der Gewährleistung des Schutzes personenbezogener Daten ausdrücklich begrüßt. „Unternehmen in der gesamten EU werden zunehmend die Vorteile erkennen, die mit dem Einsatz eigener Hüter der Privatsphäre verbunden sind“, betont Rechtsanwalt Christoph Klug von der Gesellschaft für Datenschutz und Datensicherheit (GDD). „Die Datenschutzbeauftragten werden dazu beitragen, den Datenschutz zu effektivieren, unnötige administrative Hürden zu beseitigen und das Vertrauen von Kunden und Mitarbeitern zu stärken“, fährt Klug fort. Dr. Sachiko Scheuing von der niederländischen Datenschutzorganisation NGFG fügt hinzu: „Der positive Einfluss der Tätigkeit von Datenschutzbeauftragten ist bereits durch eine Studie des niederländischen Justizministeriums belegt. Wir begrüßen daher ihre ausdrückliche Anerkennung auf Europäischer Ebene.“

Auch mit Blick auf den nach dem Verordnungsentwurf möglichen Sanktionsrahmen, der im Fall von Datenschutzverstößen durch Unternehmen bis zu zwei Prozent ihres weltweiten Jahresumsatzes reicht, dürften sich verantwortliche Stellen sicherer fühlen, wenn sie auf die Dienste eines hinreichend qualifizierten und zuverlässigen Datenschutzbeauftragten zurückgreifen können.

„Nachdem nunmehr der lang erwartete Verordnungsentwurf offiziell vorgestellt worden ist, werden die CEDPO-Mitgliedsorganisationen ihre Kräfte bündeln und den EU-Institutionen konstruktive Vorschläge für eine zukunftsfähige Ausgestaltung der Rolle des Datenschutzbeauftragten unterbreiten“, informiert Pascale Gelly von der französischen Datenschutzorganisation AFCDP. „Insbesondere wird CEDPO hierbei seine Erfahrungen aus verschiedenen EU-Mitgliedstaaten beispielsweise hinsichtlich der notwendigen Unabhängigkeit, Qualifikation und der Aufgabenstellung von Datenschutzbeauftragten insgesamt einbringen. In diesem Zusammenhang stellt CEDPO bereits heute eine vergleichende Studie zur Funktion des Datenschutzbeauftragten in 12 Mitgliedstaaten vor.“

Über CEDPO:

CEDPO wurde im September 2011 von nationalen Datenschutzorganisationen als europäischer Dachverband gegründet. Zu den Gründungsmitgliedern zählen: AFCDP (Association Française des Correspondants à la Protection des Données à Caractère Personnel), Frankreich; APEP (Asociación Profesional Española de Privacidad), Spanien; GDD (Gesellschaft für Datenschutz und Datensicherheit), Deutschland; NGFG (Nederlands Genootschap van Functionarissen voor de Gegevensbescherming), Niederlande.

CEDPO hat sich eine zeitgemäße Förderung der Rolle des Datenschutzbeauftragten und allgemein das Eintreten für einen ausgewogenen, praktikablen und effektiven Datenschutz in der EU zum Ziel gesetzt. Gleichzeitig ist CEDPO bestrebt, die Harmonisierung des Datenschutzrechts und der Datenschutzpraktiken in der EU/dem EWR zu fördern.

Quelle: GDD e.V.

Schuldnerverzeichnis im Internet: Datenschützer kritisieren elektronisches Schuldnerverzeichnis

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder übt Kritik an dem geplanten „elektronischen Schuldnerverzeichnis“. Hintergrund sind Befürchtungen hinsichtlich der Such-Maske: Dass etwa sichergestellt sein muss, dass bei gleichem Namen (es gibt mehrere Personen mit dem gleichen Namen, was nicht so unwahrscheinlich ist) von Betroffenen nicht jemand fälschlicherweise von einem Suchenden dort identifiziert wird. Hinzu kommt, dass diese Formulare eine recht weitgehende Suche ermöglichen, die Insolvenzbekanntmachungen sind da ein gutes Beispiel – um unberechtigte Massen Anfragen zu verhindern, sollen entsprechende Schutzvorrichtungen installiert werden. Insgesamt bleibt derzeit abzuwarten, wie das Formular konkret aussehen wird.

Quelle: Anwaltskanzlei Ferner Alsdorf

Aus der Welt des Tracking und des Online Behavioural Advertising

Ein neues Projekt lässt vermuten, dass Google von den Benutzern lernen möchte, wie sich diese durch das Web bewegen und wie die angesurften Seiten genau genutzt werden. Dazu hat Google das Projekt „Screenwise“ ins Leben gerufen.

Teilnehmer am Programm müssen älter als 13 sein, sich eine Erweiterung für Google Chrome installieren und werden dann getrackt. Bei der Benutzung werden die Seiten übertragen, die vom User besucht werden. Mit Hilfe dieser Profilbildung möchte Google seine Dienste verbessern. Die (teilweise) Aufgabe der Privatsphäre wird von Google für den Anfang mit einem 5 Dollar-Gutschein für Amazon entlohnt. Danach erhält der entblößte Surfer alle drei Monate, bis zu einer Maximalsumme von 25 Dollar.

Eine datenschutzkonformere Auswertung des Userverhaltens betreibt die nugg.ad AG.

Die Firma nugg.ad fungiert als Auftragnehmer, der für den Webseitenbetreiber das Nutzerverhalten aufzeichnet und auf statistischer Basis an diesen Empfehlungen für Inhalte oder Werbung

zurückliefert. Die Aufzeichnung des Nutzungsverhaltens erfolgt mit Hilfe von Cookies. Diese haben keine Identifizierungskennzeichen, sondern führen eine „Strichliste“ über die Kategorien und Art der besuchten Webseiten. Die Datenschutzkonformität wurde sogar vom ULD (Europrise) bescheinigt.

Der Targeting-Spezialist nugg.ad gab nun die Ausweitung seines Geschäfts bekannt und stellt eine Technologie vor, die dem rasant wachsenden Mobile-Display-Markt ebenfalls erfasst und damit intelligentes und systemübergreifendes Zielgruppenmanagement erstmals für Werbemaßnahmen auf mobilen Endgeräten verfügbar macht. Die Umsetzung der nugg.ad Targeting-Lösung für Mobile-Devices erfordere unter Berücksichtigung der besonderen Anforderungen im Hinblick auf den Datenschutz die Entwicklung einer gänzlich neuen Tracking-Technologie. Die nugg.ad Mobile Solutions beinhalten eine neuartige mobile-spezifische Lösung, die es erlaubt, über 90 Prozent aller mobilen Endgeräte übergreifend zu targeten, ohne dabei auf die Datenschutzkonformität zu verzichten.

Quellen: Google und nugg.ad ag

GDD-Fachtagung: Die neue EU-Verordnung zum Datenschutz

Die Auswirkungen auf den Datenschutz in Deutschland

Die EU-Kommission hat eine umfassende Reform des Datenschutzrechts in Europa vorgeschlagen. Zentrale Regelung für die Wirtschaft ist der Entwurf einer Datenschutz-Verordnung mit unmittelbarer Wirkung ohne Umsetzungsspielräume. Mit der Verordnung soll das Datenschutzrecht in Europa vereinheitlicht und die Datenschutzrechte des Bürgers gestärkt werden.

Die geplante Datenschutz-Verordnung hat auf die deutsche „Datenschutzkultur“ weit reichende Auswirkungen.

Eine Änderung der Rechtsstellung der betrieblichen Datenschutzbeauftragten, erhebliche Haftungsrisiken und der Eingriff in etablierte und bewährte Datenschutzprozesse sind nach dem Entwurf der Verordnung vorgesehen.

Die GDD-Fachtagung am 12.03.2012 in Köln informiert über die Regelungen der Datenschutz-Verordnung und beleuchtet die rechtlichen, organisatorischen und technischen Auswirkungen.

Weitere Informationen finden Sie unter www.datakontext.com

**Möchten Sie bei Erscheinen der aktuellen Datenschutz Newsbox informiert werden und so keine Ausgabe mehr verpassen?
Dann tragen Sie sich unverbindlich und kostenlos ein unter www.datakontext.com/newsletter**