ecolex
FACHZEITSCHRIFT FÜR WIRTSCHAFTSRECHT
MÄRZ 2010
03
213 – 312

ÖNorm B 2110 Ausgabe 2009

Vertragsstrafe
Leistungsbehinderung
Sicherstellung
Forcierungskosten

Haftungsausfüllung beim
Anlegerschaden

Gewährleistung beim
Unternehmenskauf

Rechtsanwalt als
Stiftungsvorstand

Diskriminierungsfreie Organisation eines
Online-Stellenmarkts

Besteuerung ausländischer
Immobilienveranlagungs-Instrumente

Online-Gaming
Regulieren statt Monopolisieren

MANZ

Die Datenschutzgesetznovelle 2010 – ein Überblick

Zum Jahreswechsel ist die lang diskutierte DSG-Nov 2010 in Kraft getreten. Mit ihr wurde das österreichische Datenschutzrecht erstmals nach zehn Jahren umfangreich reformiert. Dieser Beitrag bietet einen Überblick über die wichtigsten Neuerungen im Datenschutzrecht.

RAINER KNYRIM / GÜNTHER LEISSLER

A. Neuerungen zur Videoüberwachung

1. Gesetzlicher Anwendungsbereich

Während die Zulässigkeit einer Videoüberwachung bislang anhand der allgemeinen Grundsätze des DSG beurteilt werden musste, finden sich nunmehr in den §§ 50 a ff DSG[1]) detaillierte Regelungen.

Als „Videoüberwachung" gilt jede systematische und fortlaufende Feststellung von Ereignissen mittels Bildaufnahme- oder Bildübertragungsgeräten, wenn davon ein bestimmtes Objekt oder eine bestimmte Person betroffen ist.[2]) Diese Definition stellt eine gegenüber der bisherigen Spruchpraxis der DSK wesentliche Erweiterung dar. So hat die DSK Bildaufzeichnungen bisher nur dann als eine Verwendung personenbezogener Daten angesehen, wenn diese in der Absicht erfolgen, bestimmte Personen zu identifizieren.[3]) Auf eine solche Identifizierungsabsicht stellt der Gesetzeswortlaut nunmehr aber gerade nicht ab; den gesetzlichen Videoüberwachungsbegriff scheint vielmehr jede fortdauernde und systematische Aufzeichnung von Personen und auch Objekten (!) zu erfüllen. Wie *Dörfler* zutreffend aufzeigt, führt dies aber zu Ergebnissen (wie zB der Unzulässigkeit von Wetterkameras), die vom Gesetzgeber keinesfalls gewollt sind.[4]) Eine sinnvolle *Eingrenzung* wird daher in § 4 Z 1 zu sehen sein, wonach Daten nur dann als personenbezogen gelten, wenn die Identität des Betroffenen bestimmt oder bestimmbar ist. Diese Auslegung findet nicht zuletzt im (ebenfalls neu eingefügten) § 50 a Abs 2 Deckung, welcher die Videoüberwachung den allgemeinen Verarbeitungsgrundsätzen der §§ 6, 7 unterstellt. Da diese wiederum nur auf die Verarbeitung personenbezogener Daten Anwendung finden, ist der in § 50 a Abs 1 geregelte Anwendungsbereich der Videoüberwachung wohl nur begrenzt auf die Aufzeichnung personenbezogener Bilddaten iS einer Identifizierbarkeit der Betroffenen zu verstehen.

Dr. *Rainer Knyrim* ist Rechtsanwalt und Partner bei Preslmayr Rechtsanwälte OG; Dr. *Günther Leissler,* LL. M., ist Rechtsanwalt und Junior Partner bei Schönherr Rechtsanwälte GmbH.

1) Weitere FN ohne Gesetzeszitat beziehen sich auf das DSG 2000.
2) § 50 a Abs 1.
3) K 121.036/0014-DSK/2005.
4) *Dörfler,* Tatort Bergstation, in diesem Heft 301.

2. Zulässige Verarbeitungszwecke

Die zulässigen Einsatzzwecke einer Videoüberwachung werden in § 50 a Abs 2 taxativ aufgezählt; demnach ist eine Videoüberwachung nur zulässig, sofern dies zum Schutz eines überwachten Objekts oder einer überwachten Person oder sonst der Erfüllung rechtlicher Sorgfaltspflichten dient. Klar ist somit, dass Videoüberwachungen zum Schutz von Personen und Rechtsgütern zulässig sind; weniger klar ist, was unter „rechtlichen Sorgfaltspflichten" zu verstehen ist. Nach den EB sind darunter Rechtsvorschriften, Bescheid- oder Gerichtsauflagen zu verstehen. Tatsächlich werden „rechtliche Sorgfaltspflichten" wohl *umfassender* zu verstehen sein: Ein Testcenterbetreiber etwa, der den Testkandidaten nur durch Videoüberwachung objektive, transparente und gleichbehandelnde Testbedingungen bieten kann, wird wohl ebenfalls im Rahmen der ihn gegenüber den Testkandidaten treffenden rechtlichen Sorgfaltspflichten handeln.[5])

3. Geheimhaltungsinteressen der Betroffenen

Die Nov regelt auch Fälle, in denen die Betroffenen durch eine Videoüberwachung nicht in ihren Geheimhaltungsinteressen betroffen sein können. MaW ist in diesen Fällen die Videoüberwachung jedenfalls zulässig. Darunter fällt etwa die Zustimmung des Betroffenen oder eine allfällige gesetzliche Berechtigung zur Vornahme der Videoüberwachung, aber auch die bloße Echtzeitüberwachung. Das bedeutet, dass Videoüberwachungen jedenfalls zulässig sind, sofern die Aufzeichnungen nicht gespeichert werden. Begründet wird dies mit der durch die Echtzeitüberwachung deutlich herabgesetzten Gefährdung der Geheimhaltungsinteressen der Betroffenen. Umgekehrt wurde auch gesetzlich klargestellt, dass der Einsatz von Videokameras im höchstpersönlichen Lebensbereich der Betroffenen (zB Toilettenräume) jedenfalls unzulässig ist. Ein absolutes gesetzliches Verbot wurde darüber hinaus für die Videoüberwachung von Mitarbeitern zur Mitarbeiterkontrolle normiert.[6]) Die EB begründen dies damit, dass stets ein gelinderes Mittel zur Kontrolle der Mitarbeiter gefunden werden kann. Dieses Verbot ist allerdings *einschränkend* zu interpretieren. So wird die Videoüberwachung eines Arbeitsplatzes (zB Kassenbereiche), von der naturgemäß auch die betroffenen Mitarbeiter erfasst werden, trotzdem erlaubt sein, sofern die Überwachung Schutz- und Sicherheitszwecken, nicht aber einer Leistungskontrolle des betroffenen Mitarbeiters dient. Aber auch in anderen Bereichen wird dieses Verbot nicht in der gesetzlich statuierten Allgemeinheit anwendbar sein; Mitarbeiter, die etwa in hochsensiblen Bereichen arbeiten (wie zB der Restauration von Kunstwerken), werden wohl trotzdem zulässigerweise videoüberwacht werden können, wenn sonst keine gelindere Überwachungsmöglichkeit besteht – dies, obwohl die Kamera letztlich zu Mitarbeiterüberwachungszwecken eingesetzt wird.

Klargestellt wurde, dass ein automatisierter Bildabgleich der Aufzeichnungen mit anderen verfügbaren Bilddaten oder sensiblen Daten (zB augenscheinliche Behinderungen, Hautfarbe) verboten ist. Dadurch soll der Gefahr diskriminierender Personenauslesen vorgebeugt werden.[7])

4. Behördliches Registrierungsverfahren

Videokameras sind beim Datenverarbeitungsregister zu registrieren und im Rahmen der Vorabkontrolle prüfen zu lassen, es sei denn, die Bildaufzeichnungen werden verschlüsselt und der einzige Schlüssel bei der DSK hinterlegt.[8]) Derart verschlüsselte Aufnahmen dürfen nur in bestimmten Anlassfällen entschlüsselt werden. Der Vorteil: Werden die Aufnahmen verschlüsselt und der Schlüssel bei der DSK hinterlegt, so darf die Kamera parallel zum Registrierungsverfahren in Betrieb genommen werden. Ansonsten, dh wenn die Kamera der Vorabkontrolle unterliegt, muss vor Inbetriebnahme die Beendigung des beh Prüfverfahrens abgewartet werden.[9])

Interessant ist, dass die Mat nunmehr auch die Überwachung des eigenen Hauses oder Grundstücks zum Zweck des Eigentumsschutzes dem Videoüberwachungsbegriff des § 50 a DSG und damit der Registrierungspflicht unterstellen. Dies *widerspricht* der bisherigen Rsp der DSK, wonach derartige Aufnahmen der Ausnahmebestimmung des § 45 (Datenverarbeitung für private Zwecke) unterliegen und daher nicht meldepflichtig sind.[10]) Die EB begründen dies damit, dass nicht nur der Hausbesitzer bzw dessen Familie, sondern auch etwa Besucher mitgefilmt werden könnten. Diese Argumentation erscheint schlüssig; es bleibt abzuwarten, ob die DSK ihre bisherige Rsp in diesem Punkt trotzdem beibehält.

Keine Meldepflicht besteht hingegen bei der reinen Echtzeitüberwachung oder wenn die Aufzeichnungen bloß auf analogen Datenträgern gespeichert werden. Letzteres wird mit der beschränkten Strukturier- und Suchbarkeit auf Analogmedien gespeicherter Informationen und der damit einhergehenden beschränkten Gefährdung der Geheimhaltungsinteressen der Betroffenen begründet.[11])

Mit der Nov wurde schließlich auch normiert, dass in den Fällen des § 96 a ArbVG entsprechende Betriebsvereinbarungen zu schließen und der DSK vorzulegen sind. Interessant ist, dass das Gesetz damit nur auf „ersetzbare" Betriebsvereinbarungen Bezug nimmt. Im Umkehrschluss müssen daher „notwendige" Betriebsvereinbarungen gem § 96 ArbVG, welche gerade für Videokameras erforderlich sind, der DSK offenbar nicht vorgelegt werden.

Wichtig ist, dass die zulässige Speicherdauer des aufgezeichneten Bildmaterials mit höchstens 72 Stunden gesetzlich begrenzt wurde. Längere Speicherfristen bedürfen einer besonderen Begründung im Rahmen des Registrierungsverfahrens. Die Vi-

5) Auch der OGH judiziert in stRsp, dass etwa Sachverständige unter gewissen Umständen einer objektiv-rechtlichen Sorgfaltspflicht gegenüber Dritten unterliegen, gleichwohl dafür keine ausdrückliche gesetzliche Grundlage existiert; vgl etwa OGH 6 Ob 108/07 m.

6) § 50 a Abs 5.

7) EB zur Nov 2010.

8) § 50 c Abs 1.

9) § 18 Abs 2.

10) DSK K600.064 – 001/0002-DVR/2009.

11) EB zur Nov 2010.

deoüberwachung ist zudem in allgemein erkennbarer Form zu kennzeichnen. Darin ist auszuweisen, wer die Kameras betreibt, sofern dessen Identität nicht ohnedies offensichtlich ist.

B. Informationspflicht bei Datenmissbrauch

1. Umfang der Informationspflicht

Von der Öffentlichkeit weitgehend unbeachtet ist am 1. 1. 2010 auch eine neue Informationspflicht in Kraft getreten, die ein neuer Abs 2 a des § 24 normiert. Mit ihr wird privaten Unternehmen wie öffentlichen Stellen eine Pflicht zur Information auferlegt, sobald ihnen eine „systematische und schwerwiegende unrechtmäßige Verwendung von Daten" bekannt wird, bei der den Betroffenen Schaden droht.

In den USA ist diese Informationspflicht seit einigen Jahren als sog *„Data Breach Notification Duty"* bekannt. Auf EU-Ebene wird deren Einführung in der DatenschutzRL seit Kurzem diskutiert. Österreich hat als zweites Land in Europa[12]) eine solche Informationspflicht bereits eingeführt und nimmt dadurch zum 30-jährigen Jubiläum des DSG wieder eine Führungsrolle bei der Weiterentwicklung des Datenschutzrechts ein.[13])

Die österreichische Bestimmung ist allerdings legistisch nicht besonders geglückt. So ist etwa unklar, wann ein Datenmissbrauch „systematisch" oder „schwerwiegend" ist. Denkbar wäre, den Begriff „systematisch", wie in den Regeln zur Videoüberwachung,[14]) in eine zeitliche Komponente iS eines länger anhaltenden oder wiederholten Missbrauchs zu bringen. Möglich wäre auch, diesem den Begriff „zufällig" gegenüberzustellen: Wenn etwa ein „Hacker" in die EDV eines Unternehmens „einbricht", um dort zB Kreditkartendaten zu kopieren, geht er nicht zufällig, sondern systematisch vor.[15]) Solche Interpretationen sind aber nur soweit denkbar, als diese vom offensichtlichen Ziel des Abs 2 a, dem Betroffenenschutz, im Einzelfall gedeckt sind.

Der Begriff „schwerwiegend" kommt im DSG zwar zweimal vor,[16]) ist in diesem aber ebenfalls nicht definiert, was erhebliche Rechtsunsicherheit bei der Prüfung, ob ein die Informationspflicht auslösender Missbrauchsfall vorliegt, mit sich bringt. Ein schwerwiegender Angriff wird etwa bei einer größeren Zahl von Betroffenen, bei einem intensiven Angriff in geschützte Bereiche oder bei wiederholten Verstößen anzunehmen sein.[17])

2. Pflicht zur Verständigung

Kommt der Auftraggeber bei seiner Prüfung eines Missbrauchsfalls zum Ergebnis, dass eine Informationspflicht vorliegt, dann ist zudem unklar, was eine „geeignete" Form der Verständigung der Betroffenen ist. In den meisten Regeln in den USA[18]) und ebenso in der seit 1. 9. 2009 in Deutschland gültigen Regelung ist als Form zunächst die direkte persönliche Verständigung des Betroffenen (etwa per Brief, aber auch E-Mail, Anruf etc) vorgesehen. Wenn dies nicht möglich ist oder einen unverhältnismäßigen Aufwand bedeuten würde, kann auch per Inserat in der Zeitung,[19]) in den USA teilweise sogar mittels Schalten von Informationsspots im Fernsehen verständigt werden.

3. Ausnahmen von der Informationspflicht

Von der Informationspflicht gibt es in § 24 Abs 2 a Satz 2 zwei (alternative) Ausnahmen, nämlich wenn diese „angesichts der Drohung eines nur geringfügigen Schadens der Betroffenen einerseits oder der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert". Der Anwendungsbereich dieser beiden Ausnahmen ist ebenfalls unbestimmt; im einen Fall ist unklar, wie hoch ein Schaden sein kann, um gerade noch als „geringfügig" zu gelten.[20]) Im zweiten Ausnahmetatbestand ist unklar, ab wann die Informationskosten unverhältnismäßig wären. Es wird dem Rechtsunterworfenen daher nichts anderes übrig bleiben, als beide Ausnahmefälle im eingetretenen Missbrauchsfall anhand der konkreten Umstände, wie mögliche Betroffenenkreise, Anzahl der möglicherweise Betroffenen, Arten der möglicherweise drohenden Schäden,[21]) mögliche Schadenshöhen etc, zu beurteilen.

4. Keine Pflicht zur Meldung an die Behörde

Die österreichische DSK ist über einen Missbrauchsfall weder zu informieren noch sonst einzubinden. Dies scheint für betroffene Unternehmen im ersten Moment zwar ein Vorteil zu sein, bedeutet aber letztlich, dass Unternehmen völlig alleine beurteilen müssen, in welcher Form Betroffene über einen Missbrauchsfall geeignet zu informieren sind. Auch im Hinblick auf mögliche zivilrechtliche Haftungen wegen Verstoß gegen Schadensminderungspflichten und mögliche Haftungsfreizeichnungen von Risikoversicherungen der betroffenen Unternehmen bei Ignorieren der Informationspflicht (Schutzgesetzver-

12) Deutschland hat als erstes Land der EU eine solche Pflicht mit 1. 9. 2009 in einem neuen § 42 a dBDSG in Kraft gesetzt, s dazu etwa *Gola/Klug,* Die BDSG-Novellen 2009, RDV 2009, Sonderblg zu H 4, 4. Siehe auch *Dresner/Norcup,* Data Breach Notification Laws in Europe, Privacy Laws & Business, Report 2009.

13) Das DSG 1978 BGBl 1978/565 trat am 1. 1. 1980 in Kraft und war damals eines der ersten Datenschutzgesetze weltweit.

14) § 50 a Abs 1.

15) Siehe dazu auch *Pollirer/Weiss/Knyrim,* Sonderausgabe zum DSG (2010) § 24 Anm 16.

16) In § 30 Abs 6 und § 32 Abs 5 in Bezug auf die Einleitung von Klagen durch die DSK beim Zivilgericht gegen private Auftraggeber wegen deren schwerwiegender Datenschutzverstöße, s dazu näher bei *Dohr/Pollirer/Weiss/Knyrim,* DSG² Anm zu § 30 Abs 6 und § 32 Abs 5.

17) *Dohr/Pollirer/Weiss/Knyrim,* DSG² Anm zu § 30 Abs 6 Z 3.

18) Es haben bis dato fast alle US-Bundesstaaten eigene, im Detail jeweils unterschiedliche Regelungen dazu erlassen.

19) So ausdrücklich vorgesehen in § 42 a dBDSG.

20) So könnten für einen wohlhabenden Bankkunden zB € 50,– unbedeutend, für einen Mindestrentner hingegen keineswegs geringfügig sein.

21) Die RV zur DSG-Nov 2010 spricht von Vermögensschäden, eine Einschränkung auf solche ergibt sich aus dem Gesetzeswortlaut jedoch nicht und wäre auch widersinnig (s dazu *Pollirer/Weiss/Knyrim,* DSG² § 24 Anm 21). Es werden daher auch mögliche immaterielle Schäden zu beachten sein.

letzung!)[22]) wird hier den Unternehmen eine erhebliche Selbstverantwortung auferlegt.

Unternehmen wie öffentlichen Stellen ist daher gleichsam zu raten, einen möglichen Ernstfall nicht unvorbereitet auf sich zukommen zu lassen, sondern proaktiv Maßnahmen zu ergreifen, um auf diesen vorbereitet zu sein. Vorbereitungsmaßnahmen sind nicht nur das Durchspielen möglicher, unternehmenstypischer Risikoszenarien durch die Rechtsabteilung. Auch die gemeinsame Ausarbeitung von Notfallplänen mit verschiedenen anderen betroffenen Abteilungen, wie etwa der PR-Abteilung, der Unternehmens-IT, dem Krisenmanagement, der Geschäftsführung sowie möglicherweise betroffenen Fachabteilungen, gehört dazu.

C. Das neue vollautomatisierte Meldeverfahren

Mit der Nov wurde im DSG ein neues, vollautomatisiertes Meldeverfahren antizipiert, das durch eine V,[23]) die bis zum 1. 1. 2012 zu erlassen ist, eingeführt werden soll. Der neue § 17 Abs 1 a sieht vor, dass dann Meldungen für nicht vorabkontrollpflichtige Datenanwendungen in elektronischer Form über ein Webinterface einzubringen sind und diese nach dem neu formulierten § 20 Abs 1 *automationsunterstützt* auf ihre *Vollständigkeit und Plausibilität* zu prüfen und bei Fehlerfreiheit *sofort* zu registrieren sind. § 20 Abs 2 enthält die Möglichkeit, bei Fehlern die Meldung wie bisher in Papier einzubringen. Es bleibt abzuwarten, wie das Verf durch die zu erlassende V im Einzelnen ausgestaltet wird und ob dies fristgerecht bis 1. 1. 2012 erfolgt.[24])

D. Verschärfung des Kontroll- und Strafregimes

Der „Trend" der Nov zielt auf eine höhere Eigenverantwortung datenverarbeitender Auftraggeber. Als Ausgleich wurden die Kontroll- und Strafmechanismen des DSG verschärft. So wurde etwa die Strafbestimmung des § 51[25]) in ein Offizialdelikt umgewandelt.

Weiters wurden die Obergrenzen der Verwaltungsstrafbestimmungen in § 52 Abs 1 und 2 geringfügig auf max € 10.000,– bzw € 25.000,– angehoben, was im internationalen Vergleich immer noch sehr niedrig ist.

Zudem wurde mit § 52 Abs 2 a ein zusätzlicher Verwaltungsstraftatbestand geschaffen, der eine Strafe bis zu € 500,– für nicht fristgerechtes Beauskunften, Richtigstellen oder Löschen von Daten nach den §§ 26 bis 28 vorsieht. Wie sich diese Verwaltungsstrafe zu § 32 verhält, der zur Durchsetzung ebendieser Rechte wie bisher auch weiterhin auf den Zivilrechtsweg verweist, wird noch zu prüfen sein.

Schließlich wurde an mehreren Stellen die Kontroll- und Registerprüfungsbefugnis der DSK betont, etwa in §§ 22 a, 30 Abs 2 a, § 30 Abs 5 und 6, § 31 a. Insb ist die DSK hinkünftig berechtigt, die Weiterführung einer Datenanwendung mittels Bescheid zu untersagen, sofern der betroffene Bf eine wesentliche unmittelbare Gefährdung seiner Geheimhaltungsinteressen glaubhaft macht.[26]) Angesichts der Tragweite eines solchen Bescheids werden an die Glaubhaftmachung hohe Anforderungen zu stellen sein. Im Übrigen kommt der DSK auch die amtswegige Berechtigung zur (auch teilweisen) Untersagung einer Datenanwendung zu, sofern sie wesentliche und unmittelbare Gefährdungen von Geheimhaltungsinteressen feststellt.[27])

§ 32 Abs 7 ermöglicht es den Zivilgerichten bei Löschungs-, Widerspruchs- oder Richtigstellungsklagen, die DSK um Überprüfung der Rechtmäßigkeit der Registrierung der betreffenden Datenanwendung zu ersuchen.

E. Zusammenfassung

Die DSG-Nov 2010 ist zu begrüßen, da sie nach zehn Jahren wieder „Bewegung" in das DSG gebracht hat. Allerdings gilt es immer noch unzureichend geregelte Bereiche zu „bearbeiten" – etwa das Internet, die Kreditinformation[28]) oder den Arbeitnehmerdatenschutz.[29]) Abzuwarten bleibt auch, ob die kurz vor Beschlussfassung aus der RV gestrichenen Verfassungsbestimmungen nach Ende der „Verfassungsblockade" der Opposition „nachbeschlossen" werden. Auch auf EU-Ebene ist durch die neue, für Datenschutzrecht zuständige Kommissarin *Reding* eine Weiterentwicklung zu erwarten.

22) Siehe zur zivilrechtlichen Verantwortlichkeit und den Informationspflichten als nebenvertragliche Schutzpflichten bei *Feiler,* Data Breach Notificaton nach österreichischem Recht, MR 2009, 281 (283 f).

23) Siehe § 16 Abs 3.

24) Siehe auch bei *Kunnert,* Der Ministerialentwurf für eine DSG-Novelle 2010: Ausgewählte Probleme, jusIT 2009/50, 102 (105).

25) Datenverwendung in Gewinn- oder Schädigungsabsicht; Strafe bis ein Jahr Freiheitsstrafe.

26) § 31 a Abs 2; s auch *Jahnel,* Datenschutzrecht (2010) 515 ff.

27) § 30 Abs 6 a.

28) Der Rechtsschutz im Internet (s etwa bei *Lechner,* Datenschutz und Internet, in *Bauer/Reimer* [Hrsg], Handbuch Datenschutzrecht [2010] 209 ff) gehört im Spannungsverhältnis zur Meinungsfreiheit klarer und besser geregelt, genauso wie die Verarbeitung von Bonitätsdaten. Dadurch könnte die jüngste Entwicklung der Rsp gebremst werden, beide dieser Rechtsbereiche mit der dafür nicht geschaffenen Bestimmung des § 28 Abs 2 zu erfassen. Siehe zu den Bonitätsdaten etwa *Knyrim,* Widerspruch gegen die Datenverarbeitung in Wirtschaftsauskunfteien? ecolex 2008, 1060 oder *Dörfler,* Datenschutz: OGH auf Abwegen? exolex 2009, 636; zum Internet jüngst OLG Linz 16. 7. 2009, 3 R 101/09 g *(Koukal)* MR 2009, 306.

29) So harrt der im Entwurf der Nov aus dem Jahr 2008 enthaltene, aber in der RV wieder entfallene betriebliche Datenschutzbeauftragte weiter seiner Einführung. Weiters benötigt es dringlicher gesetzlicher Normierung des „Graubereichs" der Mitarbeiterdatenverarbeitung und Mitarbeiterkontrolle durch Datenverarbeitung im Spannungsverhältnis zwischen Datenschutzrecht, arbeitsverfassungsrechtlichen Rechten und unternehmerischen Präventions-, Kontroll- und Nachforschungspflichten.

SCHLUSSSTRICH

Die DSG-Nov 2010 brachte eine Fülle an Neuerungen im Datenschutzrecht. Unternehmen und öffentliche Stellen sind gut beraten, sich mit diesen Änderungen umfassend vertraut zu machen.