Anzeigen-Sonderveröffentlichung

DATENSCHUTZ UND SICHERHEIT IM UNTERNEHMEN

Ausbildung oder Dienstleistung von Datenschutzexperten

Es gibt viel zu tun für den Datenschutz

Unternehmen mit regelmäßig mehr als neun Beschäftigten in der automatisierten, personenbezogenen Datenverarbeitung sind verpflichtet, einen internen Datenschutzbeauftragten zu ernennen und ausbilden zu lassen oder einen externen Datenschutzbeauftragten mit den Gesetzesanforderungen zu betrauen. Der Geschäftsleitung stellt sich die Frage, ob es der faktisch unkündbare interne Datenschutzbeauftragte sein soll oder der externe Datenschutzbeauftragte, der oftmals Know-how und Apparat eines größeren Datenschutz (DS)-Dienstleisters hinter sich hat.
Die Kedua GmbH aus Berlin bedient mit DS-Ausbildung und DS-Dienstleistung beide Varianten. Die Seminarreihe zur Ausbildung von internen Datenschutzbeauftragten läuft bundesweit.
Nahezu jede Woche finden die Seminare an unterschiedlichen Orten statt. Der modular gestaltete Lerninhalt erlaubt ‚Seminar-Hopping'. Die Dozenten sind Fachleute aus der Praxis. Sie haben als externe Datenschutzbeauftragte ungefilterten Einblick in die Problemstellungen vor Ort. Fordert ein Unternehmen einen externen Datenschutzbeauftragten an, werden Aufbau und Erhalt eines gesetzeskonformen Datenschutzmanagements vom Anbieter übernommen.
Bedürfen interne Datenschutzbeauftragte fachlichen Rats, sind die Experten von Kedua ebenfalls zur Stelle. Unabhängig davon, ob es um Unterstützung für Lösungen von Teilaufgaben oder um komplexe Problemstellungen geht.
Für eine fundierte Umsetzung gesetzlicher Vorgaben erstellt Kedua Statusberichte und Datenschutzkonzepte.
Bei einer derart komplexen Materie wie dem Datenschutz werden Seminare zum Auffrischen des Kenntnisstands auch von ‚alten Hasen' gern genutzt. Darüber hinaus sorgen regelmäßig stattfindende Datenschutztage für eine kontinuierliche Weiterbildung der Datenschutzbeauftragten. Mitarbeiterunterweisungen sind als offene Seminare oder direkt in den Unternehmen als Inhouse-Veranstaltungen zu buchen. Ziel ist es, möglichst viele Mitarbeiter mit den gesetzlichen Bestimmungen vertraut zu machen, um ihr Bewusstsein für einen sensiblen und gesetzeskonformen Umgang mit Daten zu schärfen.
www.datenschutzexperten.de

BDSG-Novellierung

Update: Datenschutzrecht

Die ersten Änderungen des Bundesdatenschutzgesetzes (BDSG-Novelle II) sind zum 1. September 2009 in Kraft getreten, die BDSG-Novellen I. und III. folgen bis Mitte 2010. Für vor dem 1. Juli 2009 erhobene oder gespeicherte Daten zum Zwecke der Werbung gelten Übergangsfristen. Diese Schonfrist reicht bis zum 1. September 2012.
Von der Kanzlei Sieling waren folgende Hinweise auf die wichtigsten Änderungen zu erfahren:
- Die Datenübermittlung an Auskunfteien und die Nutzung mathematisch-statistischer Wahrscheinlichkeitswerte (Scoring) wird für den Verbraucher mehr Transparenz, für Unternehmen mehr Rechtssicherheit gewährleisten.
- Die Datenverarbeitung zu Zwecken der Werbung und des Adresshandels kann künftig – mit wenigen Ausnahmen – nur noch mit Einwilligung des Betroffenen erfolgen.
- Die Stellung des betrieblichen Datenschutzbeauftragten wurde verbessert, ein besonderer Kündigungsschutz für ihn eingeführt.
- Neuerdings besteht bei Datenschutzverstößen eine Selbstanzeigepflicht. Der Bußgeldrahmen reicht nunmehr von 50.000 Euro bis 300.000 Euro.
- Das Outsourcen von Lohnbuchhaltung oder IT-Dienstleistungen verlangt eine schriftliche 10-Punkte-Vereinbarung zwischen Auftraggeber und -nehmer.
- Der bislang vernachlässigte Teil des Arbeitnehmerdatenschutzes hat im BDSG eine neue Regelung erfahren, die nahezu ohne Veränderung der Rechtslage einhergeht.

Rechtsanwältin Carola Sieling, Fachanwältin für IT-Recht

Der Bundesminister für Arbeit und Soziales der vorherigen Regierung hatte 2009 einen Diskussionsentwurf für ein Gesetz zum Beschäftigtendatenschutz vorgelegt. Ob das Gesetzgebungsvorhaben allerdings während der jetzigen Legislaturperiode realisiert werden wird, bleibt abzuwarten.
www.kanzlei-sieling.de

Ohne Datenschutz drohen Bußgelder und Imageschäden

Datenmissbrauch
Die unterschätzte Gefahr

Der Wettbewerb unter den Marktteilnehmern in Zeiten der Wirtschaftskrise führt dazu, dass Gefahrenherde im Unternehmen wie die IT-Infrastruktur, das Kundenmanagementsystem oder die Mitarbeiterdatenverwaltung als solche nicht erkannt werden. Kommen Daten aufgrund mangelnder Absicherung abhanden oder werden sie missbräuchlich verwendet, kann das für das Unternehmen existenzbedrohend sein.

Von Seiten des Unternehmens produzierte Daten marktrelevanter Bereiche, wie die der Produktentwicklung, werden meist von vornherein unter Verschluss gehalten. Schließlich repräsentieren diese Daten die wirtschaftliche Basis des Unternehmens. Daten des alltäglichen Geschäfts hingegen ziehen in der Regel weniger Aufmerksamkeit auf sich. Auftragsdaten und Personaldaten fehlt Profitpotenzial. Trotzdem gibt es geradezu zwingende Gründe, besonders auch diese Datenaufkommen umfassend zu schützen.
Nicht nur wegen der Haftung, die bei Bekanntwerden von Datenschutzverstößen zu erwarten ist, sondern auch wegen des Ansehensverlusts bei Kunden und Öffentlichkeit.
Nach dem deutschen Datenschutzrecht sind personenbezogene Daten zu schützen. Personenbezogen sind Daten, die eine Person identifizierbar machen. Die Einhaltung der Gesetze wird durch die Aufsichtsbehörde überprüft. Im Rahmen einer Prüfung hat das Unternehmen den Beweis zu führen, dass die rechtlich vorgeschriebenen Maßnahmen getroffen wurden.
Kann der Vollzug der Verkehrssicherungspflichten nicht nachgewiesen werden, stehen nicht nur die Unternehmen sondern auch Geschäftsführer persönlich in der Haftung. Es drohen empfindliche Bußgelder, wenn der Pflicht zur Bestellung eines Datenschutzbeauftragten nicht nachgekommen wurde.
„Wir können öfter feststellen", so heißt es aus dem Beratungs-Haus Intersoft Consulting Services, „dass die Sensibilität für diese Thematik selbst in größeren Betrieben nicht immer ausreichend vorhanden ist. Erst wenn Vorgänge juristische Verwicklungen einschließlich möglicher Schadenersatzansprüche mit sich bringen, beginnt ein entschiedenes Umdenken."
Ganz allgemein sei das Risiko-Bewusstsein beim Nutzen moderner Kommunikationskanäle noch zu schwach ausgeprägt. Der positive Nebeneffekt eines Datenschutz- und IT-Sicherheitskonzeptes ist der gleichzeitige Schutz der Geschäftsdaten. Im digitalen Zeitalter muss nicht mehr das Wissen über die Bestandteile der produzierten Ware, sondern vielmehr die unternehmerische Kreativität wie zum Beispiel die Vermarktungsmethode des Produktes geschützt werden. Dieses Wissen ist oft digitalisiert und fließt in den allgemeinen Datenstrom des Unternehmens ein. Dort ist es den gleichen Risiken wie die personenbezogenen Daten ausgesetzt.
Das Hamburger Beratungs-Unternehmen Intersoft Consulting Services setzt mit seinem Angebot dort ein, wo im Unternehmen der datenschutzrechtliche Standard erreicht werden soll. Neben dem Beratungsschwerpunkt Datenschutz deckt ICS insbesondere auch die Fachgebiete IT-Sicherheit, IT-Compliance und IT-Governance ab. Ein fachübergreifendes Know-how in den Beratungsteams, meist aus Juristen, Wirtschaftsinformatikern und IT-Auditoren bestehend, erlaubt eine umfassende Analyse sowie die Entwicklung nachhaltiger Lösungsstrategien. Das partnerschaftliche Kooperationsprinzip erweist sich regelmäßig als besonders geeignet, wenn aufgrund besonderer Umstände Neuland betreten werden muss.
www.intersoft-consulting.de

Neuer biometrischer Fingerkey-Leser

Effektive Zutrittskontrolle

Für umfassende Lösungen in den Bereichen der Zutrittskontrolle und Sicherheitstechnik erregen neue biometrische Fingerkey-Leser wie der Casys wachsende Aufmerksamkeit. Ihnen werden von Herstellerseite einfache Nutzung, Robustheit und Manipulationssicherheit attestiert.
Als eines der bundesweit operierenden Systemhäuser bietet die AZS System AG umfassende Lösungen für die Bereiche Zeiterfassung, Personalinformation, Zutrittskontrolle und Sicherheitstechnik.
Gemäß Bedarf und Größe der zu sichernden Objekte erhalten die Kunden aus Industrie, Handel, Verwaltung und öffentlichem Dienst komplette Systemlösungen.
Steigende Sicherheitsanforderungen werden mit brandneuen Hard- und Software-Entwicklungen beantwortet. So hat AZS seit neuestem den biometrischen Fingerkey-Leser Casys mit den zwei Betriebsarten „Template on Card" und „Template on System" in die Systemlösungen Access 3010 integriert.

Fingerprint mit Leser

Beim Template-on-Card-Prinzip werden die Fingerdaten (Template) nur auf dem der Person zugeordneten Ausweis gespeichert. Die Kontrolle erfolgt durch Vergleich der auf dem Ausweis gespeicherten und vom Lesegerät erkannten Fingerabdrücke. Stimmen die Daten überein, führt der Terminal weitere Prüfungen durch. Werden dort keine Abweichungen festgestellt, wird der Zutritt durch Tür oder Schranke frei gegeben.
Beim Template-on-System-Prinzip werden die Fingerdaten in einer Datenbank gespeichert. Die Datenbank verteilt die Templates als Referenzmuster an die dafür ausgewählten Terminals mit Fingerkey-Leser. Die Kontrolle erfolgt durch Vergleich der Lesegerätdaten mit dem Referenzmustern. Erst nach weiteren Prüfungen und Übereinstimmungen werden Tür oder Schranke freigegeben. Casys ist für die Systeme Legic, Mifare, Hitag erhältlich, System EM wird nur „on System" bereitgestellt.
www.azs.de

Wenig Aufwand – spürbare Effizienz

Die elektronische Signatur

Das Siegel – Sicherheitssymbol für Authentizität des Originals

Mit dem Siegeszug der Informationstechnologie erwartete man das papierlose Zeitalter. Doch die Entwicklung ging in die andere Richtung. Dazu trug auch das Festhalten am traditionellen Dokument aus Papier bei. War Dokumentenstatus erforderlich, verließ man das digitale Kommunikationszeitalter und wechselte in die akribisch angelegten Ordner mit der Parallelwelt im Din A4-Format.
Diese Dopplung wollen immer mehr Unternehmen, zumindest bereichsweise, hinter sich lassen. Aus gutem Grund, schließlich ergeben sich aus der Nutzung der heute zur Verfügung stehenden Qualifizierungstechniken bedeutende Einsparpotenziale. Es geht nicht allein um die Einsparung von Kosten für Papier, Druck und Porto, beispielsweise bei Rechnungsstellung. Auch der Wegfall der Schnittstellen von einem zum anderen Medium sowie der zeitsparende elektronische Weg schlagen zu Buche. Rechnungen, die eher den Empfänger erreichen, sind eher zu begleichen.
Der Hamburger Anbieter Signable nutzt die wachsende Nachfrage nach einer effizienten elektronischen Signatur. Im Zentrum seines Angebots steht die Qualifizierte Elektronische Signatur (QES). „Aus einer im Computer erstellten Rechnung wird ganz einfach per Mausklick ein QES-gesichertes Dokument. Damit ist seine sichere Herkunft (Authentizität) und die Unversehrtheit (Integrität) seiner elektronischen Daten gewährleistet und der Inhalt rechtsverbindlich", sagt Geschäftsführer Ulrich Frotscher. Auch dem Rechnungsempfänger, also dem Kunden des Anwenders, bringen elektronisch signierte Rechnungen spürbare Vorteile. Per Mausklick kann geprüft werden, ob die Rechnung echt und unverändert ist. Gegenüber der Steuerprüfung ist der Rechnungsempfänger jederzeit in der Lage, die Echtheit einer elektronisch signierten Rechnung nachzuweisen. Laut Umsatzsteuergesetz § 14 ist die Qualifizierung Voraussetzung für die steuerliche Anerkennung von elektronischen Rechnungen. Mit Signable lassen sich außer Rechnungen auch andere Dateien signieren. Mit einer kostenlosen Software-Installation in Verbindung mit dem Signable-Service werden die angeforderten Signaturen in web-Geschwindigkeit für wenige Cent erstellt.
www.signable.de

Anwaltliche Unterstützung

Risiken sind auszuschalten

Seit September 2009 sind in vielen Unternehmen Überprüfungen des datenschutzrechtlichen Status' und infolgedessen auch manche Anpassungen erforderlich geworden. Da die DS-Problematik zunehmend an Bedeutung gewinnt, wächst der Bedarf an juristischen Bewertungen. Die kooperierenden Kanzleien der Rechtsanwältinnen Daniela Kirf-Busenbender und Nakibe Ademi bieten ihren Klienten den Beratungsschwerpunkt Datenschutz wie zum Beispiel bei: Auftragsdaten-Verarbeitung, Abklärung von Datenschutzrisiken bei internationalen Beziehungen, Datenübertragung zwischen Unternehmen, Arbeitnehmerdatenschutz und Vertragsgestaltung unter Berücksichtigung datenschutzrechtlicher Bestimmungen. Anwältin Ademi kann darüber hinaus im Balkan-Handel – vor allem mit dem Kosovo – Erfahrung und sprachliche Kompetenz einbringen.
www.anwalt.busenbender.net
www.rain-ademi.de

intersoft: consulting services

Mit intersoft consulting services - spezialisiert auf Datenschutz, IT-Sicherheit, IT-Compliance und IT-Governance - profitieren Sie von interdisziplinären Kompetenzen.

Unsere Consultants, darunter Juristen, Wirtschaftsinformatiker und IT-Auditoren, vereinen jeder für sich und im Team fachübergreifendes Know-how.

Als Hamburger Beratungshaus stellen wir unsere Kompetenzen bundesweit in den Dienst mittelständischer Unternehmen und international tätiger Großkonzerne.

Mit externen Datenschutzbeauftragten für über 80 Unternehmen gehören wir zu den führenden Dienstleistern in diesem Bereich.

Wir halten Sie auf Kurs!
www.intersoft-consulting.de

intersoft consulting services GmbH ▪ Frankenstraße 18a ▪ 20097 Hamburg
Telefon: +49 40 808108 - 0 ▪ E-Mail: info@intersoft-consulting.de

Stichworte aus dem Datenschutz (DS)-Lexikon der Kedua GmbH

Anonymisierte Daten: Sie unterfallen grundsätzlich nicht dem BDSG und können uneingeschränkt bearbeitet, genutzt und weitergegeben werden. Nach der Legaldefinition des § Abs. 6 BDSG gelten Daten dann als anonymisiert, wenn Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten Person oder einer bestimmbaren Personengruppe zugeordnet werden können.
Kompetenzen der Aufsichtsbehörde: • Anordnung zur Beseitigung von technischen oder organisatorischen Mängeln • Bei Nichtbeseitigung dieser Mängel die Untersagung von Verfahren • Verlangen der Abberufung betrieblicher Datenschutzbeauftragter, bei nicht hinreichender Fachkunde oder Zuverlässigkeit.
Auftragsdatenverarbeitung: Lässt ein Unternehmen personenbezogene Daten von Kunden, Partnern etc., aber auch der eigenen Mitarbeiter (z.B. Lohn- oder Gehaltsabrechnungen) durch ein fremdes Dienstleistungsunternehmen bearbeiten, so obliegt die datenschutzrechtliche Verantwortung weiterhin dem beauftragenden Unternehmen. Bei der Auswahl des Auftragnehmers sollte deshalb stets besonderes Augenmerk auf den dortigen Sicherheitsstandard gelegt werden. Die Auftragsvergabe muss schriftlich erfolgen und die Festlegung der Datenerhebung, ihrer Verarbeitung oder Nutzung, der technischen und organisatorischen Maßnahmen und etwaiger Auftragsverhältnisse umfassen.
Auskunftsrecht des Betroffenen: Der von der Erhebung personenbezogener Daten Betroffene kann regelmäßig Auskunft verlangen über: • die zu seiner Person gespeicherten Daten sowie deren Herkunft, • die Empfänger oder die Kategorien der Empfänger, an welche Daten weitergeleitet wurden, • den Zweck der Weiterleitung.
Darüber hinaus kann der Betroffene bei der geschäftsmäßigen Speicherung von Daten zum Zwecke der Übermittlung Auskunft über die Herkunft der Daten sowie deren Empfänger verlangen, soweit nicht das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt. Die Auskunft muss schriftlich und in der Regel unentgeltlich erteilt werden.
Außenprüfung am PC des Steuerpflichtigen
Die Änderung der Abgabenordnung (AO) sollte ab dem 01.01.2002 auch eine Außenprüfung von Buchhaltungsunterlagen des Steuerpflichtigen unmittelbar an dessen PC ermöglichen. Da hierbei lediglich die nach der AO ohnehin aufbewahrungspflichtigen Unterlagen durch den Prüfer aufgerufen und eingesehen werden dürfen, bestehen hiergegen eigentlich keine datenschutzrechtlichen Bedenken. Problematisch ist hingegen der Umstand, dass viele Unternehmen die Lohnunterlagen ihrer Mitarbeiter nicht wirksam von den sonstigen Personaldaten getrennt haben. Letztere dürfen durch den Prüfer jedoch nicht eingesehen werden. Aus diesem Grunde wurde die Neuregelung zunächst außer Verzug gesetzt. Die Unternehmen müssen jetzt dafür Sorge tragen, dass die Lohnunterlagen von den sonstigen Personaldaten getrennt gespeichert werden.
Automatisierte Erhebung, Verarbeitung oder Nutzung
Eine automatisierte Erhebung, Verarbeitung oder Nutzung dieser Daten ist immer dann gegeben, wenn Datenverarbeitungsanlagen zum Einsatz kommen.

AZS System AG

„Datenschutz & Sicherheit" in Ihrem Unternehmen

Fingerprint mit Leser und Tastatur

Wollen Sie wissen, wer wann (Zeit) und wo (Serverraum, Ihr Büro) in Ihrem Unternehmen war?

Wollen Sie verhindern, dass jeder zu jeder Zeit (nachts und am Wochenende) sich unbemerkt in Ihrem Unternehmen bewegen kann?

Wenn ja, dann entwickeln wir gern mit Ihnen eine Lösung, auch im Bereich Zeiterfassung und Personalmanagement.

Telefon 040 / 22661-1, Fax 040 / 2276753
www.azs.de

www.DATENSCHUTZexperten.de

- Stellung eines externen Datenschutzbeauftragten
- Aus- und Weiterbildung Ihres internen Datenschutzbeauftragten
- Beratungen zum Datenschutz
- Datenschutzkonzepte
- Unterweisung Ihrer Mitarbeiter im Datenschutz

KEDUA
030 43 77 86 25 @ dialog@kedua.de

IMPRESSUM

Ihr Ansprechpartner für Anzeigenaufträge:
Anzeigenverkaufsteam
Nord/Hamburg DIE WELT/WELT am SONNTAG,
Stephan Naujok, Tel.: 040/347 27 38 6, Fax: - 27 38 8,
E-Mail: media-hamburg@welt.de,
Dirk Seidel (verantw.),
Redaktion, Produktion: Günter Dahl

Sign able
Qualifizierte elektronische Signaturen
Sign.able GmbH & Co. KG
Theodorstraße 42–90, Haus 7
22761 Hamburg
Telefon 040-897 262-800
E-Mail info@signable.de
Web www.signable.de

Geschäftsführer Ulrich Frotscher

Daniela Kirf-Busenbender
Nakibe Ademi
Rechtsanwälte

- Datenschutz
- IT-Recht
- Gewerblicher Rechtsschutz
- Wettbewerbsrecht
- Arbeitsrecht
- Handels- und Gesellschaftsrecht
- Arbeitsrecht
- Verwaltungsrecht
- Insolvenzrecht

Radickestraße 29c
21079 Hamburg
Tel.: 040 / 429 00 037

Ruhrstraße 42
22761 Hamburg
Tel.: 040 / 822 97 973

www.anwalt.busenbender.net · www.rain-ademi.de