audatis INFO
Newsletter für Datenschutz + Datensicherheit in kleinen und mittleren Unternehmen

Nr. 1 B / 2012
Ausgabe 1

Was plant die EU im Datenschutz zukünftig?

Der Entwurf einer EU-Datenschutzverordnung sorgt für viele Fragen bei Unternehmen und Sorgen bei Datenschutzbeauftragten

(CR) Seitdem die EU-Kommission am 25. Januar 2012 ihren 139 seitigen Entwurf einer Verordnung "zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)" veröffentlich hat, herrscht Ungewissheit bei vielen Datenschutzbeauftragten und Unternehmen.

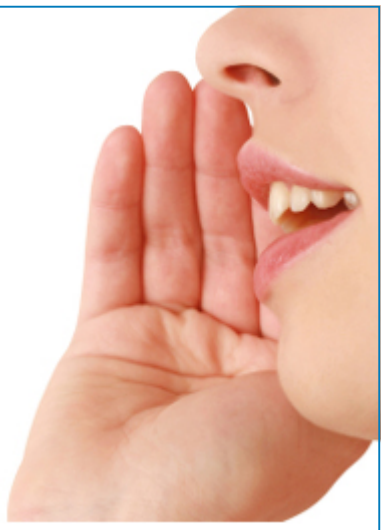
In den Medien wird eine Schwelle von 250 Mitarbeitern zitiert, ab welcher erst die Bestellung eines betrieblichen Datenschutzbeauftragten notwendig sein soll. Schon werden die ersten Fragen gestellt: "*Meine Firma hat nur 90 Mitarbeiter und fällt damit unter die 250 Mitarbeiter-Regelung der EU. Brauche ich jetzt keinen Datenschutzbeauftragten mehr bzw. gilt die Verordnung für mich dann nicht mehr?*". Ein anderer Unternehmer freut sich: "*Ich kann nun die Kosten für meinen externen Datenschutzbeauftragten einsparen, da wir keine 250 Mitarbeiter haben!*".

Doch leider ist dies etwas zu kurzfristig gedacht bzw. zu schnell gefreut. Denn wer nun davon ausgeht, dass die EU-Verordnung ab nächster Woche auch für deutsche Unternehmen gilt, hat sich leider getäuscht.

In der Tat hat die EU-Kommission zwar einen entsprechenden Entwurf für eine EU-weit gültige Datenschutzverordnung vorgestellt. Allerdings handelt es sich nur um einen ersten Entwurf und selbst in diesem wird eine Einführungsphase für die Jahre 2014 – 2016 erwartet (siehe Seite 122 des EU-Entwurfs). Sollte es noch weitere Änderungen oder Beschwerden geben – wovon auszugehen ist – wird das Verfahren noch länger dauern.

Es gilt also hierzulande weiterhin das deutsche Bundesdatenschutzgesetz (BDSG) mit all seinen Anforderungen und Auflagen bis mindestens 2014 oder 2016. Ebenfalls sind auch weiterhin die deutschen Aufsichtsbehörden für die Kontrolle des Datenschutzes und der Einhaltung des Gesetzes zuständig… (*Fortsetzung auf Seite 3*)

audatis
Datenschutz und Informationssicherheit | NEWSLETTER



Bleiben Sie auf dem Laufenden mit unserem Newsletter!

http://ds-its.eu/info

IN DIESEM NEWSLETTER

EU-Datenschutz Entwurf..... 1
Adresskartei für Werbung ... 2
EU-Datenschutz Entwurf 3
Risiken und Bußgelder..... 3
Veranstaltungen 2012 / 1.... 4
Mitarbeiter sensibilisieren.... 4
Fachkunde notwendig..... 4
Mobile Sicherheit 5
Online-Services..... 6
Aufbewahrungsfristen 6
Impressum 6
Kontaktmöglichkeiten..... 6

IM NÄCHSTEN NEWSLETTER

Videoüberwachung im Betrieb
Veranstaltungen 2012 / 2
Aktuelle Themen
Sicherheit + Cloud Computing

Ist Ihre Adresskartei ab September noch legal?

(CR) Am 31. August 2012 läuft die Übergangsfrist aus, die der Gesetzgeber bei der Novellierung des Bundesdatenschutzgesetzes (BDSG) im Jahr 2009 vorgesehen hat. Wer seine Kundendatei bis dahin nicht "sauber" hat, läuft Gefahr seine Daten löschen zu müssen. Auch geht er das Risiko ein, von den Aufsichtsbehörden mit Bußgeldern belegt oder wegen Wettbewerbsverstößen belangt zu werden.

Der Gesetzgeber hat im Rahmen der Novellierung des BDSG auch die Nutzung von personenbezogenen Daten für eigene Geschäftszwecke (wie z.B. Werbung) in §28 BDSG neu geregelt und strengere Auflagen als bisher festgesetzt. In §28 Abs. 3 ff. BDSG werden die Voraussetzungen festgelegt, welche zur Verwendung der Adressen für Werbezwecke erfüllt sein müssen:

- Die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke der Werbung ist zulässig, soweit der Betroffene eingewilligt hat. (§28 Abs. 3 BDSG)
- Sofern keine schriftliche Einwilligung vorliegt, hat die verantwortliche Stelle dem Betroffenen den Inhalt der Einwilligung schriftlich zu bestätigen. (§28 Abs. 3a BDSG)
- Wurde die Einwilligung elektronisch abgegeben, muss diese protokolliert und jederzeit abrufbar sein. (§28 Abs. 3a BDSG)
- Außerdem muss der Betroffene die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen können. (§28 Abs. 3a BDSG)

Darüber hinaus gibt es in §28 Abs. 3 Nr. 1-3 BDSG noch einige "Erleichterungen" auf deren Grundlage die adressierte Briefwerbung auch ohne Einwilligung zulässig ist:

- Bei den Adressaten handelt es sich um eigene Bestandskunden
- oder die Adressen stammen aus allgemein zugänglichen Verzeichnissen (z.B. Telefonbuch, Branchenverzeichnis, …).
- Die Werbung richtet sich nicht an Verbraucher, sondern nur an Adressaten im Hinblick auf deren berufliche Tätigkeit unter der beruflichen Anschrift.
- Spendenwerbungen einer steuerbegünstigten Organisation sind ebenfalls zulässig.

Sofern ein Adressat von seinem Widerspruchsrecht nach §28 Abs. 4 BDSG gebrauch macht oder bereits in der Vergangenheit gemacht hat, ist eine Nutzung seiner Daten zu Werbezwecken in jedem Fall unzulässig.

Für Sie als werbetreibendes Unternehmen bzw. verantwortliche Stelle ist nun relevant, dass Sie im Fall einer Prüfung z.B. durch die Aufsichtsbehörden nachweisen können, auf welcher Grundlage Sie die Berechtigung zur Nutzung Ihrer Kundendaten begründen.

Haben Sie Daten von potentiellen Kunden bereits vor dem 1.9.2009 erhoben und ohne deren Einwilligung gespeichert (welche Sie belegen sollten) müssen Sie diese vor der Verwendung auf die obigen "Erleichterungskriterien" hin prüfen.

Sind diese erfüllt, können Sie die Daten auch weiterhin für Werbezwecke verwenden.

Sollten Sie allerdings feststellen, dass die Einwilligung für den Zweck der Werbung fehlt bzw. nicht belegt werden kann und die Datenerhebung bzw. -nutzung auch nicht durch die erleichternden Kriterien abgedeckt sind, haben Sie bis zum 31.08.2012 noch die Möglichkeit die Einwilligung nachzufordern.

Dabei müssen Sie den Adressaten anschreiben und ihm unter Bezugnahme auf den gewünschten Zweck (z.B. die Verwendung seiner Daten zur Werbung) die Notwendigkeit seiner Einwilligung erklären.

Sofern der Adressat einwilligt (am besten schriftlich) können die Daten auch weiterhin genutzt werden.

Verweigert der Adressat die Einwilligung oder fordert er die Löschung seiner Daten, so müssen Sie diesem Wunsch nachkommen.

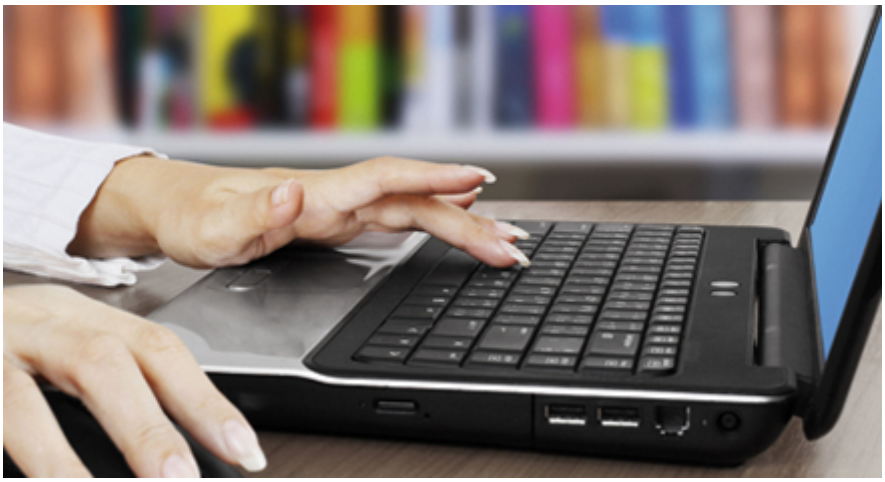
"Wie kann ich meine bisher gesammelten Adressen auch in Zukunft für eigene Werbezwecke wie z.B. Mailings nutzen?"

Alleine schon zur Minimierung Ihres Risikos bei der Verwendung von Kundendaten ab dem 01. September 2012, sollten alle Datensätze gelöscht oder zumindest gesperrt werden, die nicht auf Grundlage eines der hier genannten Verfahren verifiziert wurden bzw. bis dahin noch legalisiert werden können.

Beachten Sie hierbei auch unbedingt alle bei Ihnen bisher eingegangenen Widerrufsforderungen.

Sollten Sie einen Betroffenen trotz dessen Widerruf zur Nutzung seiner Daten für Werbezwecke versehentlich" anschreiben, kann sich dieser mit der unrechtmäßigen Verwendung seiner Daten an die Aufsichtsbehörden wenden. Diese wären dann zur Prüfung verpflichtet und könnten dabei noch weitere Fälle bei Ihnen entdecken. Die Aufsichtsbehörden können im günstigsten Fall die Löschung der Daten fordern oder aber Bußgelder in Höhe von 50.000 EUR und mehr verhängen.

Nach den Regeln des BDSG ist es im Übrigen unerheblich, in welcher Form Sie Ihre Datensätze speichern (CRM, Excel, Papierliste, …) das BDSG gilt immer.



Fortsetzung von Seite 1

Die EU-Datenschutzverordnung

… Nachdem also feststeht, dass die Einführung und Umsetzung dieser Verordnung noch eine ganze Weile dauern wird, bleibt die Frage was denn aus den internen oder externen Datenschutzbeauftragten wird, die nach §4f BDSG bestellt wurden.

In der geplanten EU-Verordnung ist die Bestellung eines Datenschutzbeauftragten (DSB) erst ab 250 Mitarbeitern Pflicht – sofern sich dies nicht noch einmal ändert.

Allerdings müssen die gesetzlichen Anforderungen an den Datenschutz (z.B. technische und organisatorische Maßnahmen) sowohl des BDSG, wie auch die einer später gültigen EU-Verordnung, unabhängig vom DSB eingehalten werden.

Damit kann der DSB in Unternehmen < 21 Mitarbeitern (aktuell) bzw. < 250 Mitarbeitern (evtl. zukünftig) somit zwar offiziell "entbehrlich" sein. Um die datenschutzkonforme Umsetzung der gesetzlichen Anforderungen aus BDSG, TMG, TKG, etc. muss sich dann aber ein anderer Mitarbeiter kümmern. Denn die Verantwortung und das entsprechende Risiko durch Datenschutzpannen, Imageschäden und Bußgelder trägt die Geschäftsführung (verantwortliche Stelle) alleine.

Da sich die Datenschutzregelungen jedoch nicht nur auf das BDSG oder eine EU-Verordnung sondern auch auf andere Gesetze beziehen (hier auch nationale Gesetze wie z.B. das deutsche Strafgesetz, Telemediengesetz, Sozialgesetz, Arbeitszeitgesetz, Arbeitsschutzgesetz …), werden weiterhin sehr komplexe Sachverhalte vorliegen, die es einem ungeschulten Mitarbeiter vermutlich sehr schwer machen werden, diese im Sinne der Risikominimierung und "Compliance" für das Unternehmens korrekt umzusetzen.

Im Zweifelsfall ist dann eben kein "Datenschutzbeauftragter" sondern ein "Datenschutzberater" gefragt, der die einzelnen Abteilungen berät und bei der Umsetzung der Anforderungen unterstützt. Alternativ kann auch ein Mitarbeiter durch entsprechende Schulungen und Weiterbildungen an die Aufgaben herangeführt werden. Ob dieser dann "Datenschutzbeauftragter" wird oder nicht – ist Entscheidung des Unternehmens.

Im Rahmen des Risikomanagements betrachten viele Unternehmer gerne auch die datenschutzbezogenen Bußgeldvorschriften (siehe Info-Kasten zu Risikomanagement und Bußgeldern rechts), sollten sich hier jedoch nicht „verkalkulieren".

Da sich die EU-Verordnung bei den Maßnahmen teilweise an der strengen deutschen Gesetzgebung orientiert – sind Unternehmen, die momentan schon nach dem deutschen Datenschutzrecht verfahren, später auf jeden Fall gut gerüstet und müssten nicht mit großen Aufwänden für eine Anpassung rechnen.

Risiko-management und Bußgelder

Alte und neue Bußgeldsätze im Datenschutzrecht

Wer gegen die Anforderungen des BDSG verstößt und z.B. keinen Datenschutzbeauftragten bestellt, obwohl er laut Gesetz dazu verpflichtet ist kann im Regelfall mit einem Bußgeld bis 50.000,- EUR, bei schwereren Vergehen bis 300.000 EUR und darüber hinaus rechnen.

In dieser Hinsicht versucht die entworfene EU-Verordnung mehr "Dampf zu machen" und erhöht die Bußgelder in drei Staffeln auf 250.000 EUR, 500.000 EUR und 1.000.000 EUR bzw. bis zu 2% des weltweiten Umsatzes des betroffenen Unternehmens.

Nach den neuen Vorschlägen sollten sich auch die Risikomanager unter den Unternehmern fragen, ob es sich "rechnet" auf Datenschutz zu verzichten und diese doch schmerzlichen Bußgelder in Kauf zu nehmen. Vom Imageschaden einmal ganz abgesehen.

Durch die Höhe der Bußgelder gilt nach wie vor die alte Regel "Datenschutz ist Unternehmensschutz" – denn ein Bußgeld kann schnell existenzbedrohend werden, obwohl nur "fahrlässig" personenbezogene Daten unrechtmäßig verarbeitet wurden und ein unzufriedener Kunde, Mitarbeiter oder Wettbewerber dies bei den Aufsichtsbehörden anzeigt.

Link zur EU-Verordnung:

http://ds-its.eu/eudsvo

Ihre Mitarbeiter sensibilisieren

Nach Ansicht vieler Experten ist die größte Schwachstelle in einer Organisation der Mensch. Diese Ansicht teilen auch wir von audatis Training und möchten Ihnen durch entsprechende Sensibilisierungsvorträge bei der Schulung Ihrer Mitarbeiter hin zu mehr Interesse und Verständnis für Datenschutz und IT-Sicherheit verhelfen.

Im Rahmen dieser sog. Security Awareness Veranstaltungen starten wir meist mit einem Live-Hacking um die Risiken am „lebenden Objekt“ und für jedermann nachvollziehbar zu demonstrieren. Anschließend werden Themen, je nach Bedarf in Ihrem Unternehmen, zur Prävention oder Erkennung von Sicherheitsvorfällen praxisbezogen referiert.

Bei Interesse kontaktieren Sie uns für ein individuelles Angebot unter:
training@audatis.de

Schulungen im eigenen Haus

Unternehmen stehen oftmals vor dem Problem Ihre Mitarbeiter zu schulen und trotzdem das Tagesgeschäft nicht aus den Augen zu verlieren. Da sind Reisezeiten und Fahrtkosten manchmal teurer, als den Trainer ins Haus zu holen.

Je nach Seminar kommen wir ab 5 Teilnehmern gerne zu Ihnen ins Unternehmen und halten die Schulung in Ihren Räumlichkeiten ab. Das spart Reisezeit und –kosten und ist vor allem bei halbtägigen bis eintägigen Veranstaltungen sehr zu empfehlen. Fragen Sie uns.

Veranstaltungen 2012 / 1

Im **Bereich Datenschutz** finden folgende Veranstaltungen zwischen **Februar und April 2012** statt:

13.02. **Datenschutzbeauftragter TÜV (W)**
in Hannover [**dsbtuv**]

29.02. **Datenschutzauditor TÜV (W)**
in München [**dsatuv**]

01.03. **Datenschutz der Personalarbeit BITKOM (O)**
online [**ds103**]

19.03. **Datenschutzbeauftragter TÜV (W)**
in Köln [**dsbtuv**]

26.03. **IT-Grundlagen für Datenschutzbeauftragte TÜV (W)**
in Köln [**dsitg**]

27.03. **Datenschutztage (F)**
in Osnabrück [**ds273**]

28.03. **Datenschutzauditor TÜV (W)**
in Köln [**dsatuv**]

16.04. **Datenschutzbeauftragter TÜV (W)**
in Leipzig [**dsbtuv**]

24.04. **Datenschutztage FFD (F)**
in Wiesbaden [**ds244**]

Für die Sparte IT-Sicherheit konnten wir folgende Veranstaltungen für Sie zwischen Februar und April finden:

26.03. **IT-Security-Beauftragter TÜV (W)**
in Hamburg [**isbtuv**]

23.04. **BSI IT-Grundschutz (W)**
in Regensburg [**is234**]

23.04. **IT-Security-Beauftragter TÜV (W)**
in München [**isbtuv**]

(F) = Fachtagung / Forum
(O) = Online / Webinar
(W) = Weiterbildung / Seminar

Sie finden **weitere Informationen** zu den Veranstaltungen und die Veranstalter über folgenden Shortlink: **http://ds-its.eu/CODE** dabei ersetzen Sie den CODE durch den entsprechenden Wert in [eckigen Klammern], welcher unter jedem Veranstaltungshinweis steht.

Fachkunde für den Datenschutz

(CR) Das Bundesdatenschutzgesetz (BDSG) fordert in §4f Abs. 2 von Datenschutzbeauftragten die erforderliche Fachkunde und Zuverlässigkeit als Voraussetzung für eine Bestellung und Übernahme dieser Aufgaben. Die Fachkunde kann nach Meinung der obersten Aufsichtsbehörden nur durch eine sachgerechte Ausbildung und regelmäßige Weiterbildung erworben bzw. aufrechterhalten werden. Somit sollte das Unternehmen schon zur Vermeidung von Bußgeldern darauf achten, dass der aktuelle oder zukünftige Datenschutzbeauftragte sich entsprechend fortbildet und dies im Zweifelsfall z.B. durch Bescheinigungen der Ausbildungsstelle nachweisen kann. Die hierfür anfallenden Kosten hat nach §4f Abs. 3 BDSG das Unternehmen zu tragen.

Ein weiterer Punkt aus dem BDSG ist die Aufgabe des Datenschutzbeauftragten, die Mitarbeiter laut §4g Abs. 2 mit den Vorschriften in geeigneter Weise vertraut zu machen. Den größten Lerneffekt haben die Mitarbeiter in der Regel bei Unterweisungen vor Ort. Sehr beliebt sind mittlerweile auch Webtrainings (eLearning) zu diesen Themen. Allerdings sind viele Produkte sehr textlastig, nicht zeitgemäß aufbereitet und somit oft eine Fehlinvestition, da der Nutzer zwar die Antworten für den Test auswendig kennt, sich aber nicht mit dem Inhalt vertraut gemacht hat.

Gerne unterstützen wir Sie bei der Auswahl der geeigneten Schulungen.

Mobile Sicherheit im Betrieb

(CR) Die Verbreitung von mobilen Endgeräten und die Nutzung des Mobilfunknetzes als Internetzugang nimmt rasant zu. Nach einer Studie des Strategieunternehmens Gartner sollen bereits in 2013 die Hälfte aller Internetnutzer auch über mobile Geräte auf das Internet zugreifen.

Die sehr leistungsstarken Smartphones und Tablet-PC sind fast immer und überall nutzbar und vereinen Handy, PC, MP3-Player, Kamera und Navi in einem einfach bedienbaren Gerät. Kein Wunder also, dass immer mehr Mitarbeiter diese Geräte auch im Unternehmen nutzen möchten, sind sie es doch bereits aus dem privaten Umfeld gewohnt überall E-Mails zu lesen oder erreichbar zu sein.

- Ist das Gerät erst einmal in fremden Händen können mit forensischen Analysen auch bereits gelöschte Daten wiederhergestellt werden.

Trotz der zahlreichen Probleme, die der Einsatz der neuen „Lieblinge“ mit sich bringt, gibt es für (fast) alle Schwachstellen eine Lösung. Angefangen bei organisatorischen Entscheidungen und Anweisungen, was die Auswahl der Geräte und deren Verwendungszweck betrifft bis hin zu technischen Sicherheitsvorkehrungen. Dabei ist natürlich auch das verwendete Modell mit seinen individuellen Schwachstellen von Bedeutung.

“Bis 2013 werden über 50% aller Internetnutzer das Internet auch mobil nutzen. Die Risiken für Smartphones & Co. nehmen entsprechen zu.”

Doch trotz der unbestrittenen Vorteile, eröffnet die Nutzung dieser mobilen PC-Vertreter auch Gefahren für die IT -Sicherheit und letztendlich auch für den Datenschutz im Betrieb.

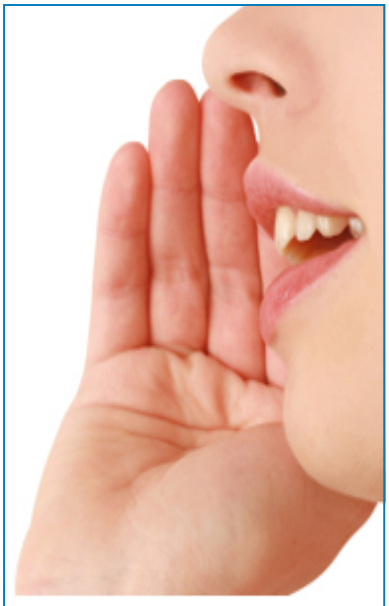
Im folgenden sind einige der aktuell bekannten Bedrohungen aufgelistet:

- Auslesen von Adressbüchern mittels Bluetooth
- Identitätsdiebstahl in manipulierten WLAN-Umgebungen
- Gespräche im GSM-Netz mithören oder SMS mitlesen
- Apps können unerlaubt Daten an Dritte übermitteln oder Schadsoftware nachladen bzw. ausführen
- Verwendung des Smartphones zur heimlichen Bewegungsüberwachung oder als Abhörwanze für Telefongespräche, aber auch Gespräche im Raum
- Auslesen von Zugangsdaten ins Firmennetzwerk und damit Zugriff auf sensible Betriebsinterna
- Die Informationen auf einem gestohlenen oder verlorenen Gerät sind teilweise schnell und einfach zugänglich

Aber egal ob als Plattform iOS (iPhone/iPad), Android oder Windows Phone zum Einsatz kommen - bei allen gibt es vor dem Einsatz einiges zu bedenken:

- Werden die Geräte einheitlich vom Unternehmen gestellt oder darf der Benutzer sein privates Gerät verwenden (auch als „Bring-Your-Own-Device“ bekannt)?
- Gibt es entsprechende Richtlinien, die den Benutzern und der IT klar vorgeben, was wer mit welchem Gerät wie machen darf?
- Kommt eine zentrale Verwaltungssoftware (Mobile Device Management) zum Einsatz, welche ein Mindestmaß an Sicherheitsregeln auf dem Gerät erzwingen und prüfen kann?
- Was passiert beim Verlust der Geräte? Können diese gesperrt, gelöscht oder lokalisiert werden?

Ein paar gute Tipps, allerdings in englischer Sprache, bietet das eBook: „Securing Smartphones & Tablets for Dummies“ von Sophos, das wir gerne auf Anfrage verschicken. Eine kurze E-Mail an info@audatis.de genügt.



Unsere Online-Services für Sie

Sie setzen ein **Webanalyse-Tool** auf Ihrer Webseite ein? Dann sollte es Sie interessieren, ob dieses auch datenschutzkonform genutzt wird bzw. werden kann. Testen Sie selbst:

http://ds-its.eu/wac

Wie ist es um das Datenschutzniveau in Ihrem Unternehmen bestellt? Halten Sie die wichtigsten Vorgaben ein? Oder gibt es noch wesentliche Baustellen? Der **Datenschutz-Schnelltest** für Unternehmen liefert die Antworten in wenigen Minuten online und als PDF zum Ausdrucken:

http://ds-its.eu/dst

Aufbewahrungsfristen 2012

(KH) Jeder Gewerbetreibende ist verpflichtet, geschäftliche Unterlagen über einen bestimmten Zeitraum aufzubewahren. Man unterscheidet dabei oft Fristen von 6 und 10 Jahren.

Die Aufbewahrungsfristen richten sich häufig nach dem Steuerrecht und dem Handelsrecht. Im Bereich des Steuerrechts werden die Aufbewahrungspflichten in der Abgabenordnung (AO) geregelt, im Bereich des Handelsrechts enthält das Handelsgesetzbuch (HGB) entsprechende Vorschriften für Kaufleute. Die handels- und steuerrechtlichen Vorschriften dazu stimmen größten Teils überein, für die betriebliche Praxis sind jedoch insbesondere die steuerrechtlichen Vorschriften relevant.

Es gibt aber auch Aufbewahrungsfristen aus anderen Rechtsgebieten, so insbesondere zum Beispiel aus dem Arbeitsrecht, dem Sozialversicherungsrecht oder dem Produkthaftungsgesetz. Weiterhin gibt es hierzu eine Vielzahl von Schreiben des Bundesfinanzministeriums (BMF).

Aus Sicht des Datenschutzes ist Datensparsamkeit geboten, welche das Löschen von nicht mehr benötigten Unterlagen vorsieht. Denn durch die gesetzlichen Aufbewahrungsfristen haben Sie im Regelfall die notwendige gesetzliche Grundlage zur Speicherung von personenbezogenen Daten. Geht diese zu Ende, entfällt auch das Recht diese Daten zu speichern, sofern es keine Einwilligung der Betroffenen gibt.

Unsere Übersicht der Aufbewahrungsfristen für 2012 gibt es hier:

http://ds-its.eu/abf2012

Hat Ihnen unser Newsletter gefallen?

Dann empfehlen Sie diesen doch gerne weiter:

www.audatis.de/online/newsletter

Die nächste Ausgabe dürfen Sie in Q2 / 2012 erwarten.

Impressum

audatis - Datenschutz und Informationssicherheit
Consulting | Training | Services
Inh. Carsten Ripper

Hauptsitz / Büro Ostwestfalen:

Dreyener Str. 20
32130 Enger

Büro Rhein-Main-Neckar:

Wehrstr. 30
69488 Birkenau

Redaktion:

V.i.S.d.P. Carsten Ripper (CR)
Kerstin Hilß (KH)

Erscheinungsweise: 4 x jährlich

Kontaktmöglichkeiten

So können Sie uns zu allen Fragen oder Anregungen erreichen:

Telefon: (05224) 999 260 - 90
Telefax: (05224) 999 260 - 99

E-Mail: info@audatis.de (allgemein)
E-Mail: newsletter@audatis.de (Newsletter-Redaktion)

Internet: www.audatis.de
Facebook: www.facebook.com/audatis
Twitter: twitter.com/audatis