AUSGABE 4 / 2014

Newsletter für Datenschutz und Informationssicherheit

audatis.INFO

In dieser Ausgabe

audatis Datenschutz und Informationssicherheit | NEWSLETTER

Editorial

Im Fitnessstudio wird er gerne als Pfand für den Spindschlüssel einbehalten, beim Mietwagen-Verleiher wird er kopiert, bevor man einen Wagen ausleihen darf und auch im Hotelgewerbe wird er gerne kopiert. Sie haben es erkannt, es geht um den Personalausweis. Das sind natürlich nur 3 Beispiele für den Umgang mit dem neuen (und alten) Personalausweis. Doch die wenigsten Menschen wissen, was eigentlich zulässig ist und was nicht. Gleiches gilt übrigens auch für die Unternehmen.
Daher haben wir es uns in diesem Herbst zur Aufgabe gemacht, den Sachstand einmal zu beleuchten und aufzubereiten und dazu eine Hilfestellung „gebastelt“, die wir Ihnen gerne auf Seite 3 zur Verfügung stellen.

Carsten Knoop
Geschäftsinhaber

Der Personalausweis, seine Kopie und der Datenschutz

Häufig werden Kopien von unserem Personalausweis angefertigt. Wir haben einmal erörtert, was erlaubt ist und wie der Umgang mit diesen Daten gesetzeskonform wäre.

(ST) Bereits im Mittelalter wurden Orden, Wappen oder Zunftzeichen zur Identifikation von Personen benutzt. Der erste „richtige“ Personalausweis wurde in der alten Bundesrepublik und in West-Berlin 1951 eingeführt und hatte die Form eines Passbuches. 1987 wurde die Passbuchform durch die kunststofflaminierte Karte abgelöst. Die aktuelle Version des Personalausweises wurde 2010 eingeführt, ist scheckkartengroß und besitzt einen RFID-Chip (Chip mit Radiowellen), in dem die Personaldaten und die biometrischen Daten (Lichtbild und Fingerabdrücke) gespeichert werden. Mit ihm soll der Ausweisinhaber sicherer identifiziert werden können und der Ausweis kann für amtliche Online-Dienstleistungen sowie für Geschäfte im Internet verwendet werden.

Ausweispflicht

Eine Pflicht zum Besitz eines Personalausweises oder eines Reisepasses für deutsche Bürger ergibt sich aus § 1 Abs. 1 PAuswG, eine grundsätzliche Pflicht zum Mitführen eines Ausweises besteht hingegen nicht, jedoch handelt ordnungswidrig, wer es unterlässt, seinen Ausweis auf Verlangen einer zuständigen und berechtigten Stelle vorzulegen.

… Fortsetzung von Seite 1 zum Thema Personalausweiskopie

Häufig werden Kopien von unserem Personalausweis angefertigt. Wir haben einmal erörtert, was erlaubt ist und wie der Umgang mit diesen Daten gesetzeskonform wäre.

Dies kann also mit einem Bußgeld geahndet werden.

Legitimation durch Ausweis

Der Personalausweis findet im Geschäftsverkehr als Legitimationsdokument häufig Verwendung. Dabei sind im Umgang mit dem Personalausweis folgende Vorgänge zu unterscheiden:

1. Das Einscannen / digitale Fotografieren durch den Inhaber selbst und das anschließende Übermitteln der elektronischen Kopie.
2. Das Kopieren und Übermitteln einer Papierkopie durch den Inhaber.
3. Das Vorzeigen und Übergeben des Ausweises zur Einsichtnahme.
4. Das Einscannen / digitale Fotografieren durch die Stelle, bei der sich der Inhaber ausweist.

Zu 1: Einscannen und elektron. Übermitteln durch den Inhaber

Hat sich eine Person gegenüber einer anderen Stelle zu identifizieren (zwecks Altersnachweis o.ä.) und ist sie nicht persönlich zugegen, dann wird von ihr häufig die Übersendung einer elektronischen Kopie (Scan) verlangt. Das Scannen von Personalausweisen ist jedoch gem. §§ 14 und 20 PAuswG untersagt. Der Gesetzesbegründung entsprechend sollen demnach „weitere Verfahren z. B. die optoelektonische Erfassung („scannen“) von Ausweisdaten oder den maschinenlesbaren Bereich ausdrücklich ausgeschlossen werden.“ Und weiter heißt es: „die Vorschrift ist erforderlich, weil der Einsatz des elektronischen Identitätsnachweises zu einem automatischen Abruf von Daten (z. B. nach Übermittlung von Daten zur Anlage eines Dienstkontos) führen kann. Von der Vorschrift erfasst sind alle Formen des automatischen Abrufs, insbesondere das Scannen, Fotokopieren und Ablichten der Daten“.

Dies bedeutet, dass selbst der Inhaber den Ausweis nicht einscannen und versenden darf, um sich gegenüber anderen Stellen zu identifizieren. Das Einscannen wird vom Gesetzgeber als unzulässige Speicherung personenbezogener Daten gewertet.

Zu 2: Übermittlung einer Papierkopie durch den Inhaber

Dass das Kopieren des Personalausweises in Papierform unzulässig wäre, ist dem Gesetzeswortlaut nicht zu entnehmen. In einem Schreiben des Bundesministerium des Innern (BMI) an den Bundesbeauftragten für den Datenschutz und Informationssicherheit (BfDI) vom 1.2.2013 führt dieses aus, dass das Anfertigen von Ausweiskopien auf all jene Fälle beschränkt werden sollte, bei denen keine Identifizierung unter Anwesenden möglich ist. Dem Betroffenen ist aber auch hier die Möglichkeit der Schwärzung nicht benötigter Daten einzuräumen, da auch hier die Grundsätze der Erforderlichkeit (§ 28 Abs. 1 BDSG) und der Datensparsamkeit (§ 3a BDSG) in jedem Fall zu beachten sind.

Daten für Identitätsnachweis

Für den Nachweis der Identität sind in aller Regel Vor- und Nachname und die postalische Anschrift ausreichend. Für die übrigen auf dem Ausweis aufgedruckten Daten, insbesondere für die sogenannte Zugangsnummer, Augenfarbe und Körpergröße, die Seriennummer, das Foto und die Prüfziffer, ist hingegen die Möglichkeit der Schwärzung einzuräumen.

Die datenschutzkonforme Vernichtung der Ausweiskopie hat grundsätzlich nach erfolgter Identitätsprüfung zu erfolgen. Zur Dokumentation der Prüfung genügt in aller Regel ein Vermerk.

Unsere Leistung

Wir beraten Sie gerne bei allen Fragen zum Datenschutz und dem Umgang mit personenbezogenen Daten. Auch prüfen wir den legalen Einsatz von Personalausweisen für Sie.

Zu 3: Vorzeigen und Übergeben durch den Inhaber
Der Personalausweisinhaber darf sich mit dem Ausweis (in der Funktion eines „Sichtausweises“) gegenüber nicht-öffentlichen Stellen identifizieren und sich damit legitimieren (§ 20 Abs. 1 PAuswG), jedoch kann vom ihm „nicht verlangt werden, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben.“

Eine Abgabe des Ausweises beispielsweise in Hotels, bei der Probefahrt mit einem Auto oder als Schlüsselpfand im Fitnessstudio ist somit durch das Hinterlegungsverbot (§ 1 Abs. 1 PAuswG) untersagt.

Zu 4: Einscannen durch andere Stellen (z.B. Unternehmen)
Die Zulässigkeit des Scannens und Speicherns von Personalausweisen durch nicht zur Identitätsfeststellung berechtigter Behörden gem. § 14 i.V.m. § 20 Abs. 2 PAuswG ist wie folgt eindeutig geregelt:

„Außer zum elektronischen Identitätsnachweis darf der Ausweis durch öffentliche und nichtöffentliche Stellen weder zum automatisierten Abruf personenbezogener Daten noch zur automatisierten Speicherung personenbezogener Daten verwendet werden.“

Die Erhebung und Nutzung personenbezogener Daten aus oder mithilfe des Ausweises darf somit nur über die vorgesehenen Kanäle erfolgen. Dies sind für nicht-öffentliche Stellen der elektronische Identitätsnachweis und für berechtigte Behörden der Abruf der elektronisch gespeicherten Daten. Damit dürfen Scans oder Kopien durch private Unternehmen definitiv nicht gespeichert werden. Kein Problem ist es jedoch laut Gerichtsurteil des Verwaltungsgerichts Hannover[1] (Urteil v. 28.11.2013, Az.: 10 A 5342/11), wenn das Unternehmen sich den Personalausweis zur Identitätsfeststellung zeigen lässt oder darin enthaltene Daten (z.B. Namen, Geburtsdatum oder Adresse) herausschreibt. Weitergehende Befugnisse stehen diesen nicht zu.

Eine Ausnahme gilt für bestimmte nicht-öffentliche Stellen wie Kreditinstitute, Finanzdienstleister, Spielbanken, Immobilienmakler, Rechtsanwälte und Notare. Diese dürfen gültige, amtliche Ausweise (dazu gehören auch Personalausweise) zur Identitätsfeststellung speichern, denn für sie gilt das Geldwäschegesetz (GwG), welches sie dazu verpflichtet, vor Begründung von Geschäftsbeziehungen oder der Durchführung von Transaktionen die Identität der Vertragspartner festzustellen. Nach § 8 Abs. 1 Satz 3 GwG kann diese Aufzeichnungspflicht auch durch eine Kopie des Ausweises erfolgen. Da der Ausweis jedoch mehr Daten erhält als nach dem GwG zu erheben und aufzuzeichnen sind, können und sollen darüber hinausgehende Informationen geschwärzt werden. Auf die Möglichkeit der Schwärzung sollen Sie im Vorfeld hingewiesen werden.

Weitere Ausnahmen können bei Telekommunikationsdienstleistern u.a. per Gesetz vorliegen, werden hier jedoch nicht betrachtet.

Die Prüfung der Rechtsgrundlage und Auswahl von geeigneten Verarbeitungsprozessen ist nicht immer trivial. Wir bieten hier Hilfestellung an.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) erklärte auf Nachfrage von audatis, dass bei Abschluss eines Vertrages oder bei Reklamationen eine Ausweiskopie erstellt werden kann, wenn lediglich die dafür notwendigen Daten entnommen werden. Nach der Dateneingabe muss die Kopie umgehend vernichtet werden. Dieser hat hierzu auch eine Broschüre zum Download veröffentlicht[2].

Fazit:
Das Scannen und Kopieren von Personalausweisen ist verboten, das Kopieren von Ausweisen ist nur dann erlaubt, sofern es bspw. per Gesetz vorgesehen oder für den Abschluss eines Vertrages oder für Reklamationen erforderlich ist und hierfür nur die notwendigen Daten gespeichert werden.

Grundsätzlich sind alle Daten frühestmöglich zu schwärzen, sofern diese nicht für die Identifikation erforderlich sind.

audatis hat hierzu zwei Kopiermasken[3] entwickelt, die Ihnen als Unternehmen die Arbeit erleichtern sollen und die wir Ihnen gerne kostenfrei zu Verfügung stellen.

Verweise zum Artikel:
[1] Urteil VG Hannover:
[http://ds-its.eu/paus]
[2] Broschüre des LDI NRW:
[http://ds-its.eu/panrw]
[3] audatis Kopiermaske:
[http://ds-its.eu/pamaske]

IT-Schwachstellen und Sicherheitslücken aufdecken und beheben

Die meisten IT-Systeme sind heute direkt oder indirekt mit dem Internet verbunden. Dadurch bieten sich ungeahnte Angriffsmöglichkeiten für Hacker aus der ganzen Welt.

(CK) Die meisten IT-Systeme sind heute direkt oder indirekt (über das Firmennetzwerk) mit dem Internet verbunden. Dadurch bieten sich hier ungeahnte Angriffsmöglichkeiten für Hacker, Datendiebe, Wirtschaftsspione und andere Akteure. In vielen Unternehmen ist dies trotz der fast täglich kommunizierten Datenskandale immer noch nicht auf der Agenda der Geschäftsführer und IT-Verantwortlichen angekommen. Häufig werden gerade bei kleineren Unternehmen die „Bedeutungslosigkeit" der eigenen IT-Systeme für fremde Angreifer herausgestellt oder auf die eigene und externe IT-Kompetenz vertraut. Doch Angreifer aus der ganzen Welt nutzen automatisierte Angriffe um IT-Systeme systematisch nach Schwachstellen auszutesten. Hierbei spielen Unternehmensgröße und -inhalt keine Rolle. Es wird angegriffen, was möglich ist und erst später überlegt, wie man daraus einen Nutzen ziehen kann. Angefangen bei der Verbreitung von Schadsoftware und SPAM bis hin zu Erpressungen, Datendiebstahl und -verkauf.

Unterschätzte Komplexität

Leider unterschätzen viele Manager die Komplexität von IT-Systemen und selbst langjährige IT-Administratoren kennen nicht alle Systeme und deren Schwachstellen in- und auswendig. Zumal täglich neue Sicherheitslücken hinzukommen. Wer sich nicht tagtäglich damit beschäftigt kennt weder die aktuellsten Angriffsmuster noch deren Abwehrmöglichkeiten. Daher ist es nicht verwunderlich, dass in den meisten IT-Systemen - von der Firewall bis hin zu Webanwendungen - zahlreiche Sicherheitslücken nur darauf warten, von Dritten ausgenutzt zu werden.

Enormes Schadenspotential

Neben dem Verlust von Firmeninterna und Betriebsgeheimnissen ist natürlich auch der Abfluss von Kundendaten ein existenzbedrohendes Szenario für jede Organisation. Nebenbei drohen zusätzlich noch Ärger und Bußgelder von Seiten des Datenschutzes, wenn gegen Informationspflichten z.B. aus § 42a BDSG verstoßen wird. Auch die Haftungsrisiken der Geschäftsführung und IT-Leitung bei groben Verstößen gegen einen sicheren IT-Betrieb können unangenehm werden.

Regelmäßige Sicheheitstests

Es gilt also den Betrieb durch regelmäßige Überprüfungen abzusichern, Schwachstellen frühzeitig zu entdecken und zu beheben, bevor diese ausgenutzt werden können. Dafür hat es sich in der Vergangenheit bewährt, auch Experten aus diesem Fachgebiet hinzuzuziehen und nicht nur den „betriebsblinden Mitarbeiter" dafür einzuspannen.

Alternative zu teuren Experten

Dabei müssen es nicht immer hauptberufliche Hacker und Penetrationstester sein, die auf Schwachstellensuche in der Unternehmens-IT gehen. Bei sehr sensiblen Daten und Systemen, ist dies natürlich die beste Variante, um die Systeme abzusichern, allerdings auch die teuerste. Ein Penetrationstester kostet zwischen 900 und 2500 EUR pro Tag. Wieso sollte man also nicht zunächst einmal versuchen mit geringerem Aufwand die große Anzahl an Sicherheitslücken zu identifizieren und erst danach auf einen Experten zurückzugreifen? In der Fachwelt haben sich daher vor allem sog. „halbautomatisierte" Sicherheitsanalysen bewährt. Diese überprüfen die IT-Systeme mit den gleichen Tools und Verfahren,

"Nutzen Sie die gleichen Angriffsmethoden wie Hacker und andere Angreifer, um die offensichtlichsten Sicherheitslücken in Ihren IT-Systemen kostengünstig zu finden und abzustellen."

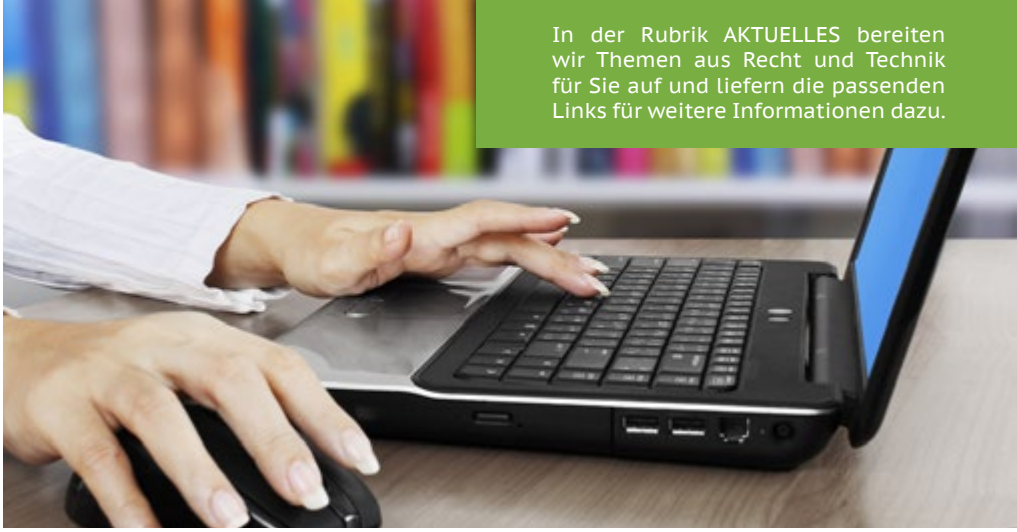
Unsere Leistung

Wir bieten Beratung bei der Auswahl passender Sicherheitsanalysen und führen diese auch regelmäßig für unsere Kunden mit erfahrenen Security-Experten durch.

wie auch ein externer Angreifer das machen würde. Werden kritische Lücken gefunden oder verspricht das Ziel besonders „lukrativ“ zu sein (z.B. größere Onlineshops) wird anschließend manuell nachgefasst.

Zwei Sicherheitmethoden

Aus diesem Grund hat audatis Consulting ein zweistufiges Konzept zur Überprüfung von IT-Systemen auf Schwachstellen entwickelt. In der ersten Stufe (BASIC) werden die beschriebenen halbautomatisierten Testsverfahren eingesetzt, um die wichtigsten Sicherheitslücken zu entdecken. Anschließend werden diese Ergebnisse durch einen Experten geprüft und der Kunde erhält einen Sicherheitsreport. Anhand dessen kann er anschließend mit den gegebenen Hilfestellungen die Probleme beheben und seine Systeme absichern. Wer noch mehr Wert auf Sicherheit legt, bekommt mit der zweiten Stufe (PREMIUM) zusätzlich manuelle Angriffe auf die Systeme sog. Penetrationstests, bei welchen der Experte seine ganze Erfahrung und Hacker-Trickkiste einsetzt. Hierdurch können auch Sicherheitslücken gefunden werden, die durch automatisierte Verfahren nicht gefunden werden können. Außerdem kann der Quellcode von Anwendungen auf Sicherheitslücken geprüft werden. Dadurch lassen sich auch Entwicklungsschwachstellen finden, die erst irgendwann in der Zukunft ausgenutzt werden können. Auf Wunsch werden die Kunden anschließend auch bei der Behebung der Schwachstellen unterstützt.
[http://ds-its.eu/pentest]



In der Rubrik AKTUELLES bereiten wir Themen aus Recht und Technik für Sie auf und liefern die passenden Links für weitere Informationen dazu.

AKTUELLES aus Recht & Technik

Personenbezug von IP-Adresse

Ob IP-Adressen personenbezogene Daten im Sinne des BDSG sind, darüber wird seit längerem gestritten. Um diese Frage zu klären, hat der BGH diese dem EuGH vorgelegt (Beschluss v. 28.10.2014, Az.: VI ZR 135/13).
Gegenstand der Diskussion ist die Frage, ob IP-Adressen einen Personenbezug aufweisen. Bei statischen IP-Adressen wird dies lt. herrschender Meinung bejaht. Strittig ist der Sachverhalt bei den dynamischen IP-Adressen, denn hier vertreten lediglich die Datenschutzaufsichtsbehörden die Meinung, dass sämtliche IP-Adressen als personenbezogenes Datum gelten.
In der praktischen Konsequenz hätte die zu treffende Entscheidung bedeutende Auswirkungen. Zum einen spielt der Personenbezug bzgl. der Problematik wie lange und unter welchen Voraussetzungen IP-Adressen gespeichert werden dürfen eine Rolle, zum anderen wird bei Analyse-Tools wie Google Analytics oder Piwik die datenschutzrechtliche Zulässigkeit an dem Personenbezug der IP-Adresse festgemacht. Gäbe es keinen Personenbezogen, müssten die deutschen Aufsichtsbehörden Ihre Vorgaben für eine beanstandungsfreie Nutzung dieser Tools ändern.
[http://ds-its.eu/ipeugh]

Sicheres Instant-Messaging

Das kostenlose Versenden von Nachrichten über Instant Messenger ist eine beliebte Alternative zu SMS und E-Mail. Doch wie steht mit der Sicherheit? Die Electronic Frontier Foundation (EFF), eine Organisation zum Datenschutz, hat die beliebtesten Messenger auf Herz und Nieren überprüft und das Ergebnis in einer übersichtlichen Tabelle aufbereitet:
[http://ds-its.eu/ismess]

Tipps für Smart-TV

Das Bundesamt für Sicherheit in der Informationstechnik hat hilfreiche Tipps zum Umgang mit internetfähigen Fernsehern („Smart-TV“) herausgebracht. Diese Geräte sind besonders geeignet, in die Privatsphäre der Nutzer einzugreifen. Bei Tests hat sich gezeigt, dass teilweise persönliche Daten verschickt werden, ohne dass der Nutzer die entsprechenden Funktionen aktiviert hatte.
[http://ds-its.eu/bsistv]

Unsere Seminare zum Datenschutz ab 2015 auch als Webinar buchbar

Für viele Arbeitnehmer wird die Zeit für Weiterbildungen immer knapper. Wir haben daher einen Teil unserer Seminare nun auch als gekürzte Webinare im Angebot.

(JB) In Zeiten knapper Kassen und immer mehr Arbeitslast in den Betrieben fällt die Bereitschaft von Arbeitgebern zur Weiterbildung der Mitarbeiter leider immer kürzer aus. Doch das ist nur eine kurzfristige Ersparnis und birgt langfristig die Gefahr - nicht mehr „up-to-date“ zu sein und in wichtigen Bereichen den Anschluss zu verlieren. Diesem Trend möchten wir entgegenwirken und Ihnen daher auch kostengünstige Alternativen zu Präsenzveranstaltungen anbieten. Nachdem wir in 2013 und 2014 nun erfolgreich die ersten Webinare durchgeführt haben, konnten wir einen hohen Zuspruch sowie sehr zufriedene Teilnehmer verzeichnen. Daher haben wir uns enschlossen, in 2015 weitere Inhalte ins Programm aufzunehmen und damit die bewährten Präsensseminare und Workshops mit neuen Webinarformaten zu ergänzen.

Einstieg oder Vertiefung

Besonders zur Weiterbildung in speziellen Bereichen können unsere Webinare ab sofort als Einstiegs- oder Vertiefungsmodule gebucht werden. Als kompletter Neueinsteiger in einem Thema bieten wir Ihnen die Webinare „Datenschutz im Personalwesen“ sowie „Datenschutz für IT-Experten“ an. Zur Vertiefung und Aufrechterhaltung der Fachkunde (gem. § 4f BDSG) bieten

wir Ihnen wie bisher „Aktuelles im Datenschutz“ sowie nun auch „IT-Sicherheit für Datenschutzbeauftragte“ mit regelmäßig wechselnden Inhalten an.

Rahmenbedingungen

In jeweils 2 x 2 Stunden erhalten Sie eine erstklassige Inhaltsvermittlung durch einen erfahrenen Referenten und können diesem natürlich - wie in einem Seminar auch - Fragen per Chat oder Mikrofon stellen. Neue Inhalte werden per Whiteboard oder Livedemo veranschaulicht, so dass die Zeit am Rechner genauso kurzweilig ist, wie vor Ort. Außerdem erhalten Sie ausführliche Unterlagen in digitaler Form sowie eine Teilnahmebescheinigung.

Technische Voraussetzungen

Um an unseren Webinaren mit der Software adobe Connect teilnehmen zu können, benötigen Sie eine Internetverbindung, einen aktuellen Internetbrowser sowie ein Headset oder Lautsprecher. Diese Voraussetzungen können Sie auf jeder Webinar-Beschreibungsseite vor einer Buchung testen.

Preise und Gutscheine

Die Webinare mit 4 Stunden Schulung durch unsere Experten kosten 199 EUR. Als treuer Leser mit dem Gutscheincode: **GS2015NW** bei Buchung bis 31.03.15 **nur 159 EUR**.

audatis Training

Wir bieten Ihnen bundesweit Fachseminare zu aktuellen Themen aus Datenschutz und Datensicherheit an. Dabei versprechen wir Ihren Erfolg mit einer Zufriedenheitsgarantie.

Der audatis Shortlink

Sie finden weitere Informationen zu den Veranstaltungen auf der rechten Seite und die jeweiligen Veranstalter über unseren Shortlink-Service:

http://ds-its.eu/SHORTCODE

*Dabei ersetzen Sie den **SHORTCODE** einfach durch den entsprechenden Wert in [**eckigen Klammern**], welcher unter jedem Veranstaltungshinweis steht und geben diesen in die Adresszeile Ihres Internet Browsers ein.*

Weiterbildung ist ein wichtiger Bestandteil der betrieblichen und persönlichen Entwicklung. Hier listen wir qualitativ hochwertige Angebote auf.

Veranstaltungstermine Dezember 2014 - März 2015

Ausgewählte Seminare und Webinare zu den Themen Datenschutz und Datensicherheit von Dezember 2014 bis März 2015 im gesamten Bundesgebiet.

Termin	Veranstaltungsbeschreibung	Ort / Uhrzeit / Shortlink
01.12.	Webinar: Aktuelles im Datenschutz [Vertiefung] (audatis Training)	Online, 09:00 - 17:00 Uhr (2x2 Std.) [wbdsa]
14.01.	Seminar: Datenschutz für IT-Leiter und IT-Experten (audatis Training)	Köln, 09:00 - 17:00 Uhr [dsitl]
20.01.	Webinar: Datenschutz im Personalwesen [Einstieg] (audatis Training)	Online, 10:00 - 16:00 Uhr (2x2 Std.) [wbdsp]
21.01.	Webinar: Sicherheit von Content-Managm.-Syst. (CMS) (audatis Training)	Online, 10:00 - 16:00 Uhr (2x2 Std.) [wbcms]
26.01. bis 27.01.	Seminar: IT-Sicherheit für Datenschutzbeauftragte (audatis Training)	Köln, 09:00 - 17:00 Uhr [itsds]
02.02. bis 04.02.	Ausbildung zum betrieblichen Datenschutzbeauftragten (Forum Fachseminare FFS)	Leipzig, 10:00 - 17:00 Uhr [semdsb]
09.02. bis 11.02.	Ausbildung zum betrieblichen Datenschutzbeauftragten (Forum Fachseminare FFS)	Stutgart, 10:00 - 17:00 Uhr [semdsb]
17.02.	Webinar: Datenschutz für IT-Experten [Einstieg] (audatis Training)	Online, 10:00 - 16:00 Uhr (2x2 Std.) [wbdsie]
18.02.	Webinar: IT-Sicherheit für Datenschutzbeauftragte [Einstieg] (audatis Training)	Online, 10:00 - 16:00 Uhr (2x2 Std.) [wbitsds]
10.03. bis 11.03.	Workshop: Grundlagen der IT-Forensik praxisnah (audatis Training)	Berlin, 09:00 - 17:00 Uhr [wksitf]
23.03. bis 25.04.	Ausbildung zum betrieblichen Datenschutzbeauftragten (Forum Fachseminare FFS)	Köln, 10:00 - 17:00 Uhr [semdsb]

Nächstes Mal

Die nächste Ausgabe des audatis.INFO Newsletters für Datenschutz und Informationssicherheit erscheint Anfang Q1 / 2015.

Einige Auszüge aus den Themen der nächsten Ausgabe:

- Software und eLearning für Datenschutzbeauftragte
- Aktuelle Veranstaltungen zu Datenschutz und Datensicherheit

Haben Sie eigene Themenvorschläge für die nächste Ausgabe(n), dann freuen wir uns über Ihre Post: newsletter@audatis.de

Datenschutz-Tools für Ihre Webseite

(CK) Seit einigen Jahren bietet audatis auf seiner Webseite bereits zwei Datenschutz-Tools an, welche Sie ab sofort auch in Ihren eigenen Webauftritt einbinden können.

Mit unserem **Datenschutz-Schnelltest** können vor allem kleinere Unternehmen, Freiberufler und Selbständige die wesentlichen Bausteine des Datenschutzes in Ihrem Hause prüfen und erhalten Hinweise auf die notwendigen Umsetzungsanforderungen z.B. ob ein Datenschutzbeauftragter benötigt wird, oder nicht.

Unser **Webanalyse-Check** überprüft die eingegebene Webseite auf den Einsatz von Webanalyse-Tools, Social-Plugins und Werbenetzwerke, welche u.U. datenschutzrechtlich bedenkliche Übermittlungen an andere Webserver im In- und Ausland unbemerkt durchführen. Zusätzlich erhalten Sie eine Information, ob Impressum und Datenschutzerklärung vorliegen und somit einen „Datenschutz-Status“ von 1 (schlecht) bis 5 (vorbildlich) Sternen.

Bisher konnten diese Tools nur auf unserer Webseite genutzt werden. Nun haben wir diese zum Einbinden via „iFrame“ auf Ihrer Webseite in einer neutralen Version vorbereitet. Hier gibt es Tools + Anleitung: [http://ds-its.eu/dstools]

Impressum

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

Wittekindstr. 3
32051 Herford

Redaktion
V.i.S.d.P. Carsten Knoop (CK)
Jill Bohrenkämper (JB)
Sebastian Treptow (ST)

Erscheinungsweise
4 x jährlich

Carsten Knoop
Geschäftsinhaber, Datenschutzauditor, Sachverständiger
Fon: 05221 85496 - 90
Mail: carsten.knoop@audatis.de

Jill Bohrenkämper
Assistentin der Geschäftsleitung
Fon: 05221 85496 - 92
Mail: j.bohrenkaemper@audatis.de

Sebastian Treptow
Wirtschaftsjurist, Datenschutzbeauftragter
Fon: 05221 85496 - 93
Mail: s.treptow@audatis.de