AUSGABE 2 / 2014

Newsletter für Datenschutz und Informationssicherheit

audatis.INFO

In dieser Ausgabe

audatis® Datenschutz und Informationssicherheit | NEWSLETTER

Editorial

In den vergangenen Monaten waren Themen rund um internationale Datenskandale und Abhöraktivitäten fast täglich in den Medien zu lesen. Der Datenschutz ist hierbei im Regelfall auf der Strecke geblieben. Häufig zu unrecht. Doch bei Aktivitäten von Geheimdiensten und rechtswidrigen Angriffen durch Hacker, wird diese Frage wohl nur selten ernsthaft gestellt.

Aber auch für den täglichen Datentransfer zwischen Unternehmen, sind Gesetze zum Datenschutz einzuhalten, um sich den Anforderungen von Compliance & Co. zu stellen und Bußgelder zu vermeiden. Welche das sind, lesen Sie in dieser Ausgabe.

Carsten Knoop
Geschäftsinhaber

Internationaler Datenschutz - was dabei zu beachten ist?

Wer personenbezogene Daten ins Ausland übermittelt, kann im Paragrafendschungel schnell die Übersicht verlieren. Wir zeigen, welche rechtlichen Aspekte für Sie wichtig sind.

(ST) Beim Umgang mit personenbezogenen Daten spielen Landesgrenzen heute kaum noch eine Rolle. Dies hängt damit zusammen, dass die Anbieter von Hard- und Software zu einem großen Teil aus international aufgestellten Konzernen bestehen, die ihren Hauptsitz in den USA oder in asiatischen Ländern haben und dort die Daten der Kunden zentral verarbeitet werden. Ebenso ist auch die stark exportorientierte deutsche Industrie global tätig und damit der Anteil der Daten von Arbeitnehmern und Kunden, die aus Deutschland in andere Länder oder von dort nach Deutschland „bewegt“ werden, entsprechend hoch. Damit der internationale Datenschutz wirksam sein kann, sind internationale Regelungen erforderlich. Auf europäischer Ebene wurde diesbezüglich eine entsprechende EU-Datenschutzrichtlinie verabschiedet, welche sich auch auf das Bundesdatenschutzgesetz (BDSG) ausgewirkt hat. Ein globales Abkommen steht dagegen noch in weiter Ferne. Damit der Schutz der Persönlichkeitsrechte auch im internationalen Geschäftsverkehr gewahrt bleibt, sind für Datenverarbeitungen, die nicht ausschließlich im Geltungsbereich des Bundesdatenschutzgesetzes stattfinden, einige Besonderheiten zu be-

… Fortsetzung des Artikels von Seite 1 zum Internat. Datenschutz

Wer personenbezogene Daten ins Ausland übermittelt, kann im Paragrafendschungel schnell die Übersicht verlieren. Wir zeigen, welche rechtlichen Aspekte für Sie wichtig sind.

achten, denn wenn eine Daten verarbeitende Stelle (bspw. Ihr Unternehmen) personenbezogene Daten in einen anderen Staat übermittelt, trägt sie die Verantwortung dafür, dass diese Übermittlung die Persönlichkeitsrechte der betroffenen Person nicht verletzt. Vermeidbare Folgen wären hier z.B. hohe Bußgelder.

Wichtige Fragen vorab

Es gilt dabei regelmäßig zwei Fragen zu klären: Welches nationale Datenschutzrecht ist auf eine Verarbeitung personenbezogener Daten anwendbar und wie wird der Schutz der Persönlichkeitsrechte bei der Übermittlung von Daten ins Ausland gewährleistet?

Anwendbares Recht im EWR

Grundsätzlich ist das BDSG anzuwenden, wenn personenbezogene Daten in den Grenzen der Bundesrepublik Deutschland erhoben, verarbeitet oder genutzt werden. Erfolgt die Datenverarbeitung durch andere Stellen, die im Europäischen Wirtschaftsraum (EWR) ansässig sind - neben den EU-Staaten gehören dazu auch Island, Norwegen und Liechtenstein - ist gem. § 1 Abs. 5 BDSG das Bundesdatenschutzgesetz nur anzuwenden, wenn die Verarbeitung durch eine Niederlassung im Bundesgebiet erfolgt. Mit dem Begriff Niederlassung ist jede effektive und tatsächliche Ausübung einer Daten verarbeitenden Tätigkeit mittels einer festen Einrichtung in Deutschland gemeint. Ein französisches Meinungsforschungsinstitut, welches in Deutschland Befragungen durchführt, ist demnach an das französische Datenschutzrecht gebunden. Wird die Befragung von einer in Deutschland niedergelassenen Stelle des Meinungsforschungsinstituts durchgeführt, ist das BDSG anzuwenden.

Rechtslage außerhalb EWR

Anders sieht die Rechtslage für Daten verarbeitende Stellen aus, die außerhalb des Europäischen Wirtschaftsraums Daten erheben, verarbeiten oder nutzen. Für sie ist gem. § 1 Abs. 5 BDSG grundsätzlich das BDSG anzuwenden. Dies allerdings mit der Einschränkung, dass dies nur auf solche Verarbeitungen Anwendung findet, bei denen die Daten verarbeitende Stelle auf Mittel zugreift, die sich in Deutschland befinden. Die Stelle hat dabei einen inländischen Vertreter zu benennen.

Zulässigkeit

Die Zulässigkeit der Übermittlung personenbezogener Daten von einem Staat in den anderen ist das Kernthema des Internationalen Datenschutzes. Die klassische Problemlage ist dabei folgende: Daten werden in einem Staat mit einem entwickelten Datenschutz verarbeitet und sollen in einen anderen Staat übermittelt werden, in dem kein oder nur ein schwächerer Schutz besteht. Der Betroffene ist somit in seinen Rechten eingeschränkt. Grundsätze wie Zweckbindung und Erforderlichkeit (beides Voraussetzungen für die Zulässigkeit) beim Umgang mit personenbezogen bezogenen Daten sind weithin unbekannt. Dieses Problem kann der nationale Gesetzgeber nicht lösen, er kann lediglich die Bedingungen für eine Ausbringung der Daten verschärfen. Daher trägt grundsätzlich die Daten verarbeitende Stelle, die personenbezogene Daten aus Deutschland heraus an eine Stelle in einem anderen Staat übermittelt, die Verantwortung. Je nach Grundlage der Datenübermittlung und in welchen Staaten die Daten übermittelt werden, sind unterschiedliche Anforderungen zu beachten.

Erlaubnis

Zunächst muss geprüft werden, ob eine Datenübermittlung gemäß § 4 Abs. 1 BDSG durch ein Gesetz erlaubt ist

Unsere Leistung

Wir beraten Sie gerne bei allen Fragen zum internationalen Datenverkehr und können Sie bei der Erstellung und Prüfung von Vereinbarungen zum Datenschutz unterstützen.

7 Schritte zur int. Datenübermittlung

1. **Anwendbares Recht prüfen:** Ist das BDSG oder ein ausl. Datenschutzgesetz anzuwenden?
2. **Zulässigkeit der Datenübermittlung prüfen:** Hier sind die Zweckbindung und Erforderlichkeit der Datenübermittlung zu prüfen. Für welchen Zweck müssen welche Daten übermittelt werden und sind auch alle übermittelten Daten dafür erforderlich?
3. **Besteht eine Erlaubnis zur Übermittlung:** Durch Gesetz oder Einwilligung (§ 4 Abs. 1 BDSG)?
4. **Übermittlung in einen Staat im EWR:** Problemlose Übermittlung, wenn der Staat zum EWR gehört.
5. **Übermittlung in einen sicheren Drittstaat:** Problemlose Übermittlung, wenn die EU-Kommission den Staat als datenschutzfreundlich eingestuft hat.
6. **Übermittlung in die USA:** Derzeit noch problemlose Übermittlung an Unternehmen, die vom US-Handelsministerium als sicher zertifiziert wurden (Safe-Harbor).
7. **Übermittlung in einen nicht sicheren Drittstaat:** Beachten Sie bitte unbedingt § 4c BDSG. Sie können z.B. die EU-Standardverträge verwenden um den Schutz der personenbezogenen Daten zu garantieren. Alternativ können Sie auch individuelle Verträge abschließen oder ein konzernweites Regelwerk (BCR) mit Garantien für die Rechte der betroffenen Personen bei der Datenverarbeitung im Konzern festlegen. Beide Alternativen müssen jedoch von der Aufsichtsbehörde genehmigt werden.

Fragen oder Probleme bei der Prüfung oder Vertragsgestaltung? Wir helfen Ihnen gerne persönlich weiter: info@audatis.de

oder ob die von der Übermittlung Betroffenen Personen Ihrer Einwilligung gemäß § 4a BDSG erteilt haben.

Staaten im EWR

Ist dies zu bejahen, ist in einer zweiten Prüfungsstufe das angemessene Datenschutzniveau im Zielstaat zu prüfen. Die von der Übermittlung Betroffenen Personen dürfen durch die Weitergabe ihrer Daten keine unverhältnismäßigen Eingriffe in ihre Persönlichkeitsrechte erfahren. Diese nicht zu befürchten, wenn die Daten in Staaten übermittelt werden, die ein angemessenes Datenschutzniveau besitzen. Dies ist anzunehmen, wenn Sie den Standards der europäischen Datenschutzrichtlinie genügen. Somit sind Datenübermittlungen an Stellen, die im europäischen Wirtschaftsraum ansässig sind, problemlos (§ 4b Abs. 1 Nr. 1 und 2 BDSG).

Sicherer Drittstaat

Ebenso bestehen keine Vorbehalte bei Datenübermittlungen an Stellen in solche Staaten, denen die Europäische Kommission durch eine so genannte Angemessenheitsentscheidung ein angemessenes Datenschutzniveau bescheinigt hat (§ 4b Abs. 2 S. 2 BDSG). Diese Staaten sind: Andorra, Argentinien, Australien, Kanada, Schweiz, Färöer Inseln, Guernsey, Israel, Isle of Man, Jersey und Uruguay.

Sonderfall USA

Bezüglich den USA gibt es mit der Safe-Harbor-Entscheidung eine Besonderheit, denn dort besteht grundsätzlich kein angemessenes Datenschutzniveau. US-Unternehmen, die

Die Prüfung der Rechtsgrundlage und Auswahl von geeigneten Verträgen ist nicht immer trivial. Wir bieten hier Hilfe auf in anderen Sprachen.

der Kontrolle des Handelsministeriums unterliegen, können aber die vom US-Handelsministerium verabschiedeten Datenschutzgrundsätze anerkennen und sich entsprechend zertifizieren lassen. Welche Unternehmen sich zertifiziert haben, ist in einer Liste des US-Handelsministeriums einzusehen.

Nicht sicherer Drittstaat

Werden personenbezogene Daten in einen Zielstaat ohne angemessenes Datenschutzniveau übermittelt, enthält § 4c Abs. 1 BDSG einige Tatbestände, bei denen eine Datenübermittlung ohne weitere Vorkehrungen durchgeführt werden kann. Neben der Möglichkeit der Einwilligung der Betroffenen Personen gibt es sechs weitere Tatbestände, die aber grundsätzlich restriktiv auszulegen sind, d.h., dass sie nicht zu einer Aushöhlung des Persönlichkeitsrechtsschutzes führen dürfen.

Greifen die oben genannten Erlaubnistatbestände nicht und sollen Daten dennoch in einen nicht sicheren Drittstaat übermittelt werden, muss die Daten übermittelnde Stelle in Deutschland dafür Sorge tragen, dass die von der Übermittlung betroffenen Personen Garantien für den Schutz der Persönlichkeitsrechte erhalten. Dazu stehen im Wesentlichen drei Instrumente zur Verfügung: EU Standardverträge, Individualverträge und verbindliche Konzernregelungen zum Datenschutz.

Was bei der Verschlüsselung von Daten in der Cloud zu beachten ist

Viele IT-Systeme speichern mittlerweile Daten in der Cloud, doch wer kümmert sich um die Sicherheit der Daten und was hat es mit SSL & Co. dabei auf Sich?

(CK / WK) Obwohl sich viele Unternehmen beim sog. Cloud Computing dank NSA und Edward Snowden mehr Gedanken um die Sicherheit ihrer Daten machen, nimmt die Cloud-Nutzung weiter zu. Die erhofften Vorteile wie eine kostengünstige und flexible Nutzung von Speicherkapazitäten aus dem Internet sind einfach zu groß. Manchmal ist den Unternehmen auch gar nicht wirklich bewusst, dass sie einen Cloud -Dienst einsetzen.

Das ist bei Privatpersonen nicht anders, ganz im Gegenteil. Es werden Cloud-Dienste als praktischer Datenspeicher genutzt, ohne sich weiter darüber Gedanken zu machen. Bei Webmail, Foto-Speichern im Internet oder der Ablage von Dateien in den Profilen sozialer Netzwerke ist vielen Nutzern gar nicht bewusst, dass sie dabei letztlich Cloud Computing nutzen.

Irrglaube Verschlüsselung

Cloud-Dienste werden oft nicht als solche erkannt oder als harmlose Online-Speicher interpretiert, und auch bei der Verschlüsselung gibt es falsche Vorstellungen. Viele Internetnutzer achten zwar inzwischen bei der Übertragung von Daten ins Internet auf die Kennzeichen einer Verschlüsselung, prüfen also, ob die Webadresse mit „https“ beginnt. Doch die Bedeutung dieser Verschlüsselung wird falsch eingeschätzt: Eine SSL- (Secure Socket Layer) oder TLS-Verschlüsselung (Transport Layer Security) betrifft die Übertragung zwischen dem Client (z.B. dem Browser) und dem jeweiligen Webserver, also zum Beispiel die Übertragung vom Browser zum Server eines Online-Foto-Speicherdienstes. Über die Verschlüsselung nach der Übertragung sagt https jedoch nichts aus.

Verschlüsselung gespeicherter Daten notwendig

Will man seine Daten auch nach der Übertragung vor unerlaubten Blicken und Zugriffen schützen, muss neben der Datenübertragung auch die Speicherung der Daten verschlüsselt erfolgen.

Verschiedene Cloud-Speicherdienste versprechen auch, dass die gespeicherten Daten ebenfalls verschlüsselt werden. Doch ist damit dem Datenschutz Genüge getan? Kann nun wirklich kein Unbefugter auf die privaten oder die betrieblichen Daten in einer so geschützten Cloud zugreifen? Leider ist das weiterhin möglich.

Unsere Leistung

Wir bieten Beratung bei der Auswahl passender Verschlüsselungssoftware und helfen Ihnen bei Implementierung geeigneter Maßnahmen und Software.

Wer hat den Schlüssel?

Wie Sie wissen, braucht man zur Entschlüsselung von Daten den jeweiligen Schlüssel. Anders ausgedrückt, kann jeder, der den richtigen Schlüssel hat, die Daten in der Cloud entschlüsseln, vorausgesetzt, er oder sie kann auf die Daten zugreifen, kennt also zum Beispiel das Nutzerpasswort.
Es stellt sich die Frage, wer auf die Nutzerkonten und deren Inhalte zugreifen kann und wer über die Schlüssel verfügt. Die Antwort: Ohne weitere Sicherheitsmaßnahmen könnten das der Cloud-Administrator und damit der Cloud-Provider sein. Möglich ist dies insbesondere dann, wenn man die Verschlüsselung seiner Cloud-Daten einfach dem Cloud-Anbieter überlässt. Es müssen also andere Lösungswege her, welche wir Ihnen nun vorstellen.

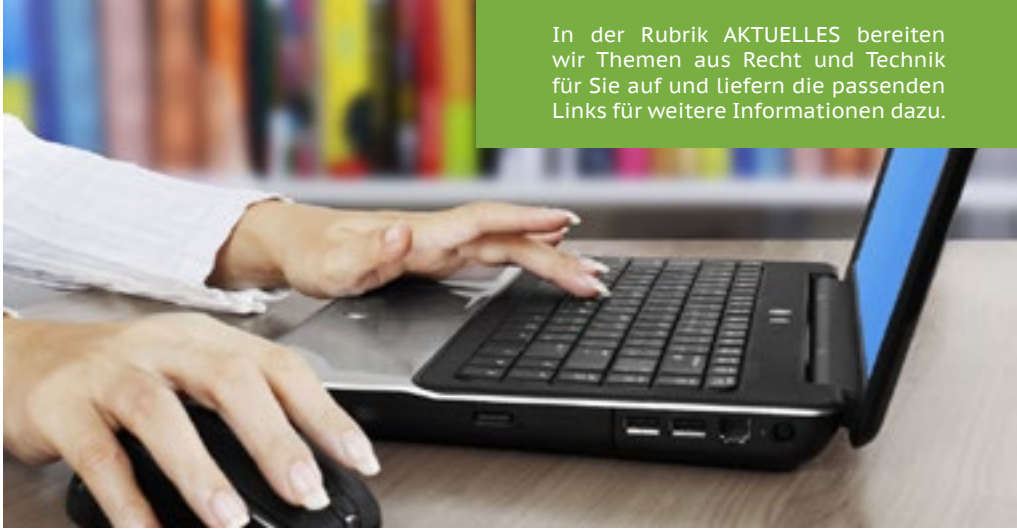
“Alleine auf den Einsatz von verschlüsselter Datenübertragung und das Versprechen von Dienstleistern zur verschlüsselten Datenspeicherung sollte man sich nicht verlassen.”

1. Selbst verschlüsseln:
Wer Cloud-Dienste nutzt und damit seine Daten einem Dritten übergibt, sollte nicht auch noch die Sicherheit der Daten anderen überlassen. Der Cloud-Anbieter sollte sehr wohl die Übertragung sowie die Speicherung der Daten seiner Kunden und Nutzer verschlüsseln. Aber die Anwender selbst sollten ihre Daten ebenfalls verschlüsseln, und zwar bereits vor der Datenübertragung in die Cloud.
Die Schlüssel für diese Verschlüsselung dürfen dem Cloud-Anbieter nicht zugänglich sein, wenn denn die Vorab-Verschlüsselung wirklich zuverlässig helfen soll. Vielmehr sollten Cloud-Nutzer ihre Schlüssel jenseits der Cloud aufbewahren, zum Beispiel auf einer Smartcard. Nur mit einer vom Cloud-Anbieter unabhängigen Verschlüsselung kann man davon ausgehen, dass kein Dritter, auch kein Mitarbeiter des Cloud-Providers, die eignen Daten einsehen kann.

2. Auswahl von Tools zur Verschlüsselung der Daten:

- Mit dem OpenSource-Tool „TrueCrypt“ verschlüsseln Sie Daten in sog. Containern, vor dem Upload. [http://truecrypt.org]
- Alternativ bietet das Tool „BoxCryptor“ sowohl privaten als auch betrieblichen Anwendern Verschlüsselungsmöglichkeiten an. [https://boxcryptor.com]
- Auch die Software „Cloudfogger“ hat sich auf Verschlüsselung für Dropbox & Co. spezialisiert. [http://cloudfogger.com]
- Die letztgenannten Dienste gibt es auch als App für Smartphones und Tablets.

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

EuGH kippt EU-Richtlinie zur Vorratsdatenspeicherung
Der EuGH hat mit Entscheidung vom 08.04.2012 (Az. C-293/12, C-594/12) die Richtlinie über die Vorratsspeicherung von personenbezogenen Daten für ungültig erklärt. Ein Eingriff von dem Ausmaß und der besonderen Schwere in die Grundrechte auf Achtung des Privatlebens und auf Schutz persönlicher Daten ist nicht gerechtfertigt, da dieser die Grenzen zur Wahrung der Verhältnismäßigkeit überschreiten würde. Gerügt wurde zudem die generelle Überwachung aller EU-Bürger, der Mangel an objektiven Kriterien zur Beschränkung durch Behörden, der Mangel an Unterscheidungen in Datenkategorien sowie fehlenden Garantien vor Missbrauchsrisiken.
[http://ds-its.eu/eughvds]

Heartbleed-Lücke sorgt für Wirbel bei der SSL-Verschlüsselung im Internet
Der Heartbleed-Exploit macht sich eine Schwachstelle in OpenSSL zunutze, über den sich schon seit längerem Daten von Servern abgreifen lassen, die SSL-verschlüsselt kommunizieren. Dabei macht sich der Heartbleed-Exploit eine Schwachstelle in der Umsetzung der Heartbeat-Erweiterung des TLS-Protokolls in OpenSSL zunutze. Erst nach und nach wird nun deutlich, wie groß der Schaden ist, der dadurch angerichtet wurde. Heise security erläutert die Angriffsmöglichkeiten und die Abwehrstrategien unter Link:
[http://ds-its.eu/heartbl]

Religionszugehörigkeit wird an Banken zur Abführung der Kirchensteuer übermittelt
Ab 2015 wird auf Kapitalerträge auch direkt von der Bank die Kirchensteuer abgeführt. Dazu müssen natürlich Daten zur Religionszugehörigkeit vorliegen. Diese kommen direkt vom Bundeszentralamt für Steuern und werden von den Banken ab Mitte des Jahres abgefragt.
Wer hier eine Verletzung seiner Persönlichkeitsrechte in Zusammenhang mit den besonderen Arten personenbezogener Daten laut § 3 Abs. 9 BDSG sieht, kann beim BzSt einen Sperrvermerk hinterlassen. Dann werden die Daten nicht mehr an die Bank übermittelt. Der Kirchensteuerpflicht ist dann gegenüber dem jeweiligen Finanzamt nachzukommen.
[http://ds-its.eu/kisteuer]

Neues Seminar: Datenschutz im Personalwesen einfach umsetzen

Unser neustes Seminar in Kooperation mit der *aconso* Academy steht für praxisorientierte Weiterbildung zu den wichtigsten Themen des Datenschutzes im Personalwesen

(JB) In allen Unternehmen und Behörden werden sensible Daten von Beschäftigten verarbeitet. Da es sich hier um personenbezogene Daten handelt, gilt es natürlich auch das Bundesdatenschutzgesetz (BDSG) einzuhalten. Von der Bewerbung über die Gehaltsabrechnung, das Führen der Personalakte bis hin zum Ausscheiden aus der Organisation, werden viele Daten erhoben und müssen gespeichert und irgendwann gelöscht werden. Doch welche Regelungen sind für Personalverwaltung und Personalentwicklung hier wirklich wichtig und wie können diese effizient umgesetzt werden?

Diese Fragestellungen werden aus Sicht der Mitarbeiter und Verantwortlichen im Personalwesen betrachtet und praxisnah vermittelt, um datenschutzkonform arbeiten und planen zu können.

Inhalte des Seminar
In unserem halbtätigen Seminar lernen Sie mit unserem Dozenten Carsten Knoop die wichtigsten Grundlagen des Datenschutzes kennen. Von der Datenerhebung bis hin zur Archivierung und Löschung werden alle Prozesse betrachtet.

Sie werden Ihr Bewerbermanagement, die Aus- und Weiterbildung von Mitarbeitern

und den Einsatz von papierbezogener und elektronischer Personalakte aus Sicht des Datenschutzes durchleuchten und praxiserprobte Maßnahmen kennenlernen, den gesetzlichen Anforderungen zu genügen.
Weiterhin werden Sie die Mitarbeiterbeurteilungen, den Einsatz von Social Media und die Gehaltsabrechnung genauer betrachten und eine datenschutzfreundliche Lösung Ihrer Problemfelder entwickeln.

Gutes Bauchgefühl inklusive
Nach Ende des Seminars sollen Sie neben den neu gewonnenen Kenntnissen und dem fundierten Wissen (auch in gedruckter Form) ein gutes Bauchgefühl mit nach Hause nehmen, was den Datenschutz in Ihrem Personalbereich angeht. Außerdem können Sie sich mit Kollegen aus dem gleichen Umfeld während eines Imbisses austauschen und eigene Fragen einbringen.

Nächster Termin und Infos:
Am 25.06.2014 findet das nächste Seminar in München statt, zu dem wir Sie gerne mit folgendem 10% Rabattcode einladen würden: perso14
Weitere Informationen zum Seminar, Anmeldemöglichkeit sowie Übernachtungsmöglichkeiten finden Sie über folgenden Shortcode:
[sempds]

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 Mai - September 2014

Ausgewählte Seminare und Fachtagungen zu den Themen Datenschutz und Datensicherheit von Mai bis September 2014 im gesamten Bundesgebiet.

Termin	Veranstaltungsbeschreibung	Ort / Uhrzeit / Shortlink
14.05. bis 15.05.	Workshop: Grundlagen der IT-Forensik praxisnah (audatis Training)	Düsseldorf, 09:00 - 17:00 Uhr [wksitf]
25.06.	Seminar: Datenschutz im Personalwesen (aconso Academy)	München, 09:00 - 14:00 Uhr [sempds]
26.06. bis 27.06.	Seminar: IT-Sicherheit für Datenschutzbeauftragte (audatis Training)	München, 09:00 - 17:00 Uhr [itsds]
	- Sommerpause von Juli bis August -	
01.09.	Webinar: Aktuelles im Datenschutz (audatis Training)	Online, 09:00 - 17:00 Uhr [wbdsa]
02.09.	Seminar: Datenschutz für IT-Leiter und IT-Experten (audatis Training)	Düsseldorf, 09:00 - 17:00 Uhr [dsitl]
02.09.	Seminar: Web-Security für Web-Entwickler (audatis Training)	Düsseldorf, 09:00 - 17:00 Uhr [wswe]
09.09.	Webinar: Sicherheit von Content-Managm.-Syst. (CMS) (audatis Training)	Online, 10:00 - 16:00 Uhr [wbcms]
10.09. bis 11.09.	Workshop: Datenschutz praxisnah und gesetzeskonform (audatis Training)	Frankfurt, 09:00 - 17:00 Uhr [dsws]
16.09. bis 17.09.	Seminar: IT-Sicherheit für Datenschutzbeauftragte (audatis Training)	Köln, 09:00 - 17:00 Uhr [itsds]
29.09. bis 01.10.	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 Ende Q3 / 2014.

Einige Auszüge aus den Themen der nächsten Ausgabe:

- Was Software für den Datenschutzbeauftragten leistet
- Datenschutz am Arbeitsplatz
- 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

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

Verstärkung im Datenschutz & IT-Recht

(CK / ST) In den vergangenen Monaten haben wir unser Büro in Herford um weitere Arbeitsplätze ausgebaut und dürfen Ihnen an dieser Stelle einen neuen Kollegen vorstellen, der sich seit März um alle Angelegenheiten des Datenschutz- & IT-Rechts kümmert.

Sebastian Treptow ist in der Niederlassung Herford / Ostwestfalen tätig. Sein Aufgabengebiet ist die kompetente und umfassende Beratung zu allen Fragen und Belangen des Datenschutzes und der Vertragsgestaltung sowie deren praktische Umsetzung.

Bevor er zu audatis kam, hat er eine Ausbildung zum Rechtsanwalts- und Notarfachangestellten abgeschlossen. Danach an der Hochschule Wismar Wirtschaftsrecht mit dem Schwerpunkt IT-Recht studiert und seinen Abschluss als Bachelor of Laws (LL.B.) erlangt. Zusätzlich ist er zertifizierter betrieblicher Datenschutzbeauftragter (FFS).

„Ich freue mich darauf, Sie kennenzulernen und mit Ihnen zuzammenzuarbeiten."

Wenn Sie Fragen zum Datenschutz haben kontaktieren Sie Ihn bitte unter den folgenden Möglichkeiten:

Telefon: 05221 85496 - 93
Mail: s.treptow@audatis.de

audatis®
Datenschutz und Informationssicherheit | NEWSLETTER

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

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