AUSGABE 3 / 2015

Newsletter für Datenschutz und Informationssicherheit

audatis.INFO

In dieser Ausgabe

audatis® Datenschutz und Informationssicherheit | NEWSLETTER

Editorial

In diesem Jahr hat sich im Sommer und Herbst einiges im Bereich Datenschutz und Datensicherheit getan.
Vom neuen IT-Sicherheitsgesetz, dass für alle Unternehmen mit Internetpräsenz neue Sicherheitsmaßnahmen fodert und von vielen unbemerkt seit August gilt, berichten wir auf Seite 5.
Viel bekannter ist das Urteil des EuGH mit den Auswirkungen auf den transatlantischen Datentransfer in die USA. Seitdem das bisher gern genutzte Safe Harbor Abkommen durch den höchsten europäischen Gerichtshof gekippt wurde, ist in vielen Unternehmen Handlungsbedarf angesagt. Wie eine zumindest temporäre Lösung aussehen kann, beschreiben wir in unserem Leitartikel.

Carsten Knoop
Geschäftsinhaber

Der (un-)sichere Hafen für die Datenübermittlung in die USA

Die Zeiten des sicheren Hafens sind vorbei – der EuGH lehnt "Safe Harbor" zum Datentransfer in die USA ab. Wir haben für Sie aufbereitet, was nun für den Datenschutz wichtig ist.

(CK) Gerade die Übermittlung personenbezogener Daten an Dienstleister in den USA stellt für viele Unternehmen eine wichtige Arbeitsgrundlage da, denn dort sitzen viele innovative Unternehmen im IT-Bereich und bieten ihre (Cloud-) Dienste über das Internet an.
Beginnend bei den Branchenriesen wie Google, Amazon, Microsoft und Facebook bis hin zu spezialisierten Anbietern wie Salesforce oder Start-ups in diversen Nischen. Auch gehören Konzernholdings und Mutterunternehmen von Unternehmensgruppen häufig zur Liste der Unternehmen mit Sitz in den Vereinigten Staaten von Amerika. Ebenso wurde ein Datentransfer von deutschen Konzernen zu deren amerikanischen Tochterunternehmen gerne über Safa Harbor abgesichert.

Zustand vor Oktober 2015

Bisher war das Outsourcing (oder eine konzerninterne Datenübermittlung) aus Sicht des Datenschutzes zumindest bei nicht besonders schützenswerten personenbezogenen Daten noch "relativ einfach" zu bewältigen, sofern die rechtliche Grundlage aus Sicht des BDSG gewährleistet war.
Bis zum 06.10.2015 konnte man sich zumindest rechtlich auf das zwischen der EU-Kommission und den USA verein-

… Fortsetzung von Seite 1 zum EuGH Urteil zu Safe Harbor

Die Zeiten des sicheren Hafens sind vorbei – der EuGH lehnt "Safe Harbor" zum Datentransfer in die USA ab. Wir haben für Sie aufbereitet, was nun für den Datenschutz wichtig ist.

barte "Safe Harbor" Abkommen verlassen, was eine freiwillige Einhaltung der europäischen Datenschutzstandards auf Seiten des amerikanischen Unternehmens - zumindest auf dem Papier - sicherstellen sollte.

Zustand seit Oktober 2015

Doch mit Datum des 6. Oktobers hat hat der Europäische Gerichtshof (EuGH) die Karten neu gemischt.

Im Rechtsstreit eines Österreichers mit Facebook hat das höchste irische Gericht *[bei welchem die Klage auf Grund des Europasitzes von Facebook in Irland anhängig war]* die Frage zur Zulässigkeit von Safe Harbor an den EuGH übergeben und dieser hat zu obigem Datum sein Urteil gefällt: *„Im Lichte von Abhör- und Ausspähskandalen wie PRISM & Co. wurde bekannt, dass u.a. von den USA regelmäßig gegen die Vorgaben des Artikel 25 Abs. 6 der EG-Datenschutzrichtlinie sowie gegen die Artikel 7 und 8 der EU-Grundrechtecharta, welche das Persönlichkeitsrecht im Allgemeinen und personenbezogene Daten im Speziellen schützen, verstoßen wurde."* Daher kann aus europäischer Sicht der Datenschutz durch diese freiwillige Verpflichtung in den USA nicht mehr gewährleistet werden. Im engeren Sinne hat der EuGH „nur" entschieden, dass einzelne nationale Aufsichtsbehörden nicht an die Entscheidungen der EU-Kommission gebunden sind und somit eigene Prüfmaßstäbe zum Datenschutz bei der Beurteilung z.B. von Safe Harbor anwenden können.

Unternehmen sind gefordert

Jetzt müssen Unternehmen schnell handeln, denn solange keine alternative Zusicherung eines angemessenen Datenschutzniveaus beim Dienstleister in den USA vorliegt, ist die Übermittlung personenbezogener Daten unzulässig. Im schlimmsten Fall könnte nun auch von deutschen Behörden ein Bußgeld verhängt werden. Dies ist zwar zunächst bis Anfang 2016 generell von den Aufsichtsbehörden nicht vorgesehen[1], kann im Einzelfall - insbesondere bei Beschwerden - jedoch eintreten. Hierbei könnten Bußgelder bis 300.000 EUR anfallen, da es sich dann um eine unrechtmäßige Datenverarbeitung handeln würde. Gem. § 38 Abs. 5 BDSG darf die Aufsichtsbehörde die Datenverarbeitung auch untersagen, was bei Nichtbeachtung mit einem Bußgeld von bis zu 50.000 EUR geahndet werden kann.

Mögliche Lösungsansätze

Nach dem Willen der deutschen Aufsichtsbehörden[1] sind jedoch auch mögliche Lösungen für das Safe-Harbor-Problem - auch zukünftig unter gleichen rechtlichen Bedingungen in den USA - unzulässig, da das Grundproblem der nicht EU-Grundrechtskonformen Überwachung durch Sicherheitsbehörden der USA weiterhin bestehen bleibt. Somit werden bis auf Weiteres keine Genehmigungen von Datenexportverträgen und verbindlichen Unternehmensregelungen (engl. Binding Corporate Rules = BCR) erteilt.

Somit verbleiben aktuell nur die EU-Standardvertragsklauseln (bis vermutlich 31.01.2016) sowie die Einwilligung für eine Datenübermittlung als Rechtsgrundlage.

Problemfall Standardvertrag

Nach Meinung der Aufsichtsbehörden stellen auch die von der EU-Kommission aufgestellten EU-Standardvertragsklauseln keine ausreichende Garantie für die Rechte der Betroffenen in den USA dar, da hier genauso wie bei Safe Harbor die Grundrechte nicht umfassend gewährleistet werden. Die Forderung einer neuen Rechtsgrundlage bis 31.01.2016 ist sportlich, wenn man den europäischen Arbeitsmodus kennt (an der EU-Datenschutzgrundverordnung wird schon seit mehr als 4 Jahren gearbeitet). Die meisten Unternehmen werden sich jedoch aktuell noch genau auf diese Rechtsgrundlage stützen müssen, sofern sie weiterhin personenbezogene Daten in die USA übermitteln möchten oder müssen.

Problemfall Einwilligung

Bei Nutzung der Einwilligung des Betroffenen wären gem. § 4c BDSG alle Probleme beseitigt, wenn nicht die Forderung nach Freiwilligkeit und Einwilligung „ohne jeden Zweifel" im Raume und zur Disposition stehen würden. Hier ist das häufigste Argument, dass der Betroffene sich der Ausmaße der Überwachung in den USA nicht bewusst sein kann und eine Einwilligung daher immer einen Hinweis auf diese Praktiken erforderlich macht. Selbst dann kann es rechtlich jedoch problematisch sein, denn sein Grundrecht auf Datenschutz darf auch per Einwilligung nicht eingeschränkt werden.

Regierungen sind aufgefordert

Am Ende werden also die Regierungen sowie deren Vertreter zwischen EU und USA neue rechtliche Grundlagen schaffen müssen, mit denen dann auch Unternehmen aus Europa eine Datenübermittlung rechtssicher durchführen können. Der Aufruf an die Gesetzgeber ist bereits adressiert.

Plan B und Restrisiko

Solange dies jedoch nicht umgesetzt und neu durchdacht wurde, trägt jedes Unternehmen das Risiko von Datenschutzverletzungen und den genannten Konsequenzen selbst. Ein möglicher Plan B kann hier nur so aussehen, dass nach Möglichkeit alle Datenübermittlungen in die USA unterbunden und durch europäische Partner, Dienstleister oder Konzernfirmen substituiert wird (auch wenn das nicht in jedem Szenario tatsächlich anwendbar sein wird).

Wie geht es weiter?

Neben dem Abschluss von EU-Standardverträgen sollten Firmen, die den Einsatz von Cloud-Dienstleistern in den USA erwägen, darauf achten, dass diese die Vorgaben der „Orientierungshilfe Cloud Computing"[2] und die „Entschließung zur Gewährleistung der Menschenrechte bei der elektronischen Kommunikation"[3] umsetzen, welche von den Datenschutzaufsichtsbehörden gefordert werden. Zudem kann jedem Unternehmen nur angeraten werden, die aktuellen Entwicklungen weiter zu verfolgen und sein Handeln danach regelmäßig zu überprüfen.

Spezialthema als Webinar

Anlässlich der zahlreichen Fragen haben wir in unserem nächsten Webinar am 17.11.15 zu diesem Thema einen besonderen Themenschwerpunkt gesetzt. [wbdsa]

Verweise zum Artikel:

[1] Positionspapier DSK: [http://ds-its.eu/shusa1]
[2] Orientierungshilfe Cloud: [http://ds-its.eu/ohcloud]
[3] Gewährleistung Menschenr.: [http://ds-its.eu/dsmenre]

Unsere Leistung

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

7 Schritte zur (US-) 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:** Beachten Sie bitte unbedingt § 4c BDSG. Derzeit nur noch Übermittlung an Unternehmen, die entweder einen EU-Standardvertrag abgeschlossen haben oder über eine gültige Genehmigung der zuständigen deutschen Aufsichtsbehörde (z.B. für BCR oder Datenexportvertrag) verfügen, welche aktuell jedoch nicht neu vergeben werden.
7. **Übermittlung in die USA durch Einwilligung:** Sie können auch eine Einwilligung des Betroffenen einholen, um die Rechtmäßigkeit sicherzustellen. Hierzu sind jedoch die strengen Vorgaben gem. § 4a BDSG zu beachten. Auf Grund der aktuellen Lage kann diese u.U. zukünftig auch unzulässig werden, sofern der Gesetzgeber dies verlangt.

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

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

Das IT-Sicherheitsgesetz und die Auswirkungen auf Unternehmen

Seitdem das IT-Sicherheitsgesetz in Kraft gesetzt wurde, haben sich still und leise einige Anforderungen für alle Unternehmen und Webseitenbetreiber eingeschlichen.

(CK) Seit dem 25. Juli 2015 gilt in Deutschland das IT-Sicherheitsgesetz. Den meisten ist dies auch aus den Medien durch die geforderten Maßnahmen für die sog. kritischen Infrastrukturen (KRITIS) bekannt. Dabei geht natürlich sehr schnell das Interesse an der Thematik verloren, wenn sich Ihr Unternehmen eben nicht zu den wichtigen Versorgungsinfrastrukturen im Land zählt. Doch das ist zu kurz gedacht.

Änderungen im TMG

In § 13 Abs. 7 TMG wurden nämlich fast unbemerkt auch Änderungen am Telemediengesetz durchgeführt, welches u.a. für jedes Unternehmen mit geschäftlicher Präsenz im Internet (z.B. Webseiten, Onlineshops, Blogs oder Apps) gilt.
Dort ist von „technischen und organisatorischen Vorkehrungen" die Rede, mit welchen „sicherzustellen ist, dass […] kein unerlaubter Zugriff […] möglich ist" und die Dienste „gegen Verletzungen des Schutzes personenbezogener Daten und gegen Störungen […] gesichert sind." – doch was bedeutet das nun für Ihr Unternehmen?

Notwendige Maßnahmen?

Bei Verstößen gegen diese neuen Verpflichtungen sieht das Gesetz ein Bußgeld bis zu 50.000 EUR vor, sofern „technisch umsetzbar und wirtschaftlich zumutbar". Was also ist jetzt umzusetzen?

1. Unerlaubter Zugriff

Unter dem „Schutz vor unerlaubtem Zugriff" gem. § 13 Abs. 7 Nr. 1 TMG fallen allgemeine Maßnahmen, die den Webserver und Webanwendungen nach außenhin absichern sollen. Ziel ist laut der Gesetzesbegründung insbesondere die Verhinderung von sog. „Drive-by Downloads" (d.h. Manipulationen einer Webseite, um bei dem Besucher ohne deren Zutun Schadsoftware zu installieren).
Hiervor können verschiedene Maßnahmen schützen:

- Regelmäßiges Einspielen von Sicherheitsupdates der verwendeten Software (inkl. Serverbetriebssystem, Datenbankanwendungen, etc.), um bekannte Schwachstellen zu schließen. Eine zeitliche Frequenz wird vom Gesetzgeber jedoch nicht vorgegeben.

Unsere Leistung

Wir bieten Beratung bei der Auswahl passender Sicherheitsvorkehrungen und führen regelmäßig Sicherheitsaudits (Penetrationstests) für unsere Kunden durch.

rung von nicht benötigten Funktionen und Zugängen.
- Einsatz geeigneter Zugriffskontrollmechanismen wie z.B. komplexe Passwörter, Sperren von Benutzern nach mehrmaliger Falschanmeldung, Verhinderung von sog. Brute-Force-Attacken zum Ausprobieren von Passwörtern.
- Durchführung von regelmäßigen Schwachstellentests (u.a. Penetrationstests), welche die Angriffsmethoden der Hacker bereits im Vorfeld ausprobieren und anschließend Maßnahmen dagegen vorschlagen.

2. Personenbezogene Daten

Mit dem „Schutz von personenbezogenen Daten" gem. § 13 Abs. 7 Nr. 2a TMG fallen vor allem Verschlüsselungsmechanismen. Dies stellt auch das Gesetz ausdrücklich in § 13 Abs. 7 Satz 3 TMG klar. Darunter ist wohl vor allem eine Transportverschlüsselung d.h. TLS/SSL zu verstehen. Dabei lässt das Gesetz jedoch auch andere Maßnahmen zu, wobei es im Endeffekt auf eine allgemeine Verschlüsselungspflicht für geschäftsmäßige Telemedien hinausläuft. Hierbei sollte folgendes beachtet werden:

"Für alle Betreiber von geschäftlichen Webseiten, Blogs oder Online-Shops gilt das neue IT-Sicherheitsgesetz mit seinen Anforderungen für die technische Absicherung dieser Webdienste."

- Einsatz von Firewalls (z.B. Web Application Firewalls = WAF) zur Absicherung von Zugriffen z.B. auf die Administrationsoberfläche.
- Systemhärtung von Server und anderen Komponenten z.B. durch Deaktivie-

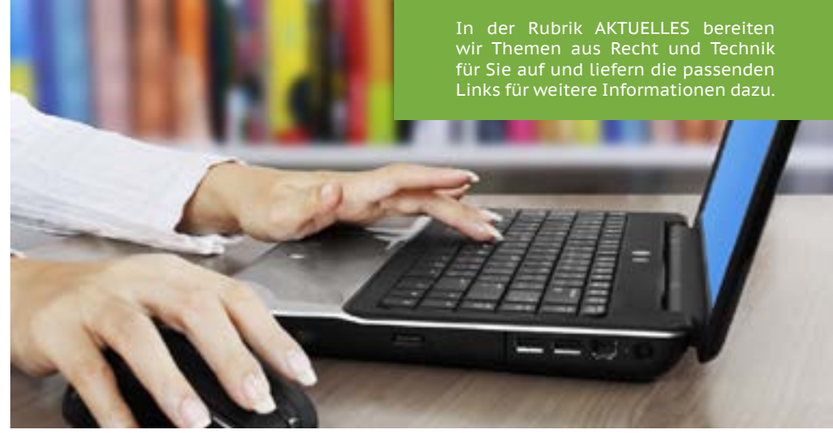
- Es muss eine sichere Verschlüsselung nach Stand der Technik eingesetzt werden. Bereits als unsicher eingestufte Verfahren sind unzulässig.
- Es muss zumindest eine verschlüsselte Übertragung (https) personenbezogener Daten erfolgen z.B. den kompletten Datentransfer der Webseite oder mindestens der Formulare verschlüsseln.
- Verschlüsselung von personenbezogenen Daten in Datenbanken (mindestens bei Bankdaten, Passwörtern, etc.).

3. Äußere Störungen

Der „Schutz vor Störungen von außen" gem. § 13 Abs. 7 Nr. 3 b) TMG wird im Gesetz offenbar mit Maßnahmen zur Abwehr von „Distributed Denial of Service"-Attacken" = DDoS, also dem gezielten Überlasten von Servern und Diensten verbunden. Details hierzu sind auch der Gesetzesbegründung nicht zu entnehmen. Jedoch wird diese Maßnahmen bei Nichteinhaltung auch nicht mit einem Bußgeld geahndet - eine Nichterreichbarkeit schädigt den Betreiber ja bereits selbst. Denkbare Maßnahmen sind jedoch:

- Einsatz von speziellen Filtern, welche Überlastungsangriffe ausfiltern können (z.B. über IP-Lokalisierung, Anzahl von Aufrufen).
- Verteilung der Last auf mehrere Rechenzentren oder Server.

Unser Service für Sie:
[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

Patientendatenschutz

Als Antwort auf eine kleine Anfrage der Linksfraktion im Bundestag hin, hat die Bundesregierung eingeräumt, dass Krankenkassen mit Wissen der Bundesdatenschutzbeauftragten regelmäßig unzulässigerweise Einsicht in sensible Krankenunterlagen nehmen, welche Ärzte an den Medizinischen Dienst (MDK) schicken. Man habe zwar keine genauen Zahlen, jedoch wurden durch Feststellungen bei Vor-Ort-Kontrollen bei Krankenkassen, Eingaben betroffener Versicherter und Informationen von Leistungserbringern der Schluss nahe gelegt, „dass es sich bei unzulässigen Einsichtnahmen durch die Kassen nicht nur um zu vernachlässigende Ausnahmefälle handelt". Als Folge soll das beanstandete „Umschlagverfahren" durch das Krankenhaus-Strukturgesetzes (KHSG) abgeschafft werden.
[http://ds-its.eu/btmdk] und [http://ds-its.eu/khsg]

Metadaten in WhatsApp

Unter anderem mit einem eigens dafür entwickelten Tool haben Wissenschaftler der Universität New Haven die Kommunikation zwischen WhatsApp und den Servern der Facebook-Tochter entschlüsselt, protokolliert und aufbereitet und zeigen in einer Untersuchung, welche Daten die neugierige App dabei durchs Netz jagt. Dabei ist insbesondere die neue Telefonfunktion sehr „gesprächig" und sendet u.a. Rufnummern, Anfang und Ende von Gesprächen an den Anbieter Facebook.
[http://ds-its.eu/whatsapp]

Videoattrappe und Betriebsrat

Nach einem Beschluss des Landesarbeitsgerichts Mecklenburg-Vorpommern besteht kein Mitbestimmungsrecht des Betriebsrates bei der Einführung einer Videoüberwachungsanlage im Unternehmen (hier Krankenhaus), wenn ausschließlich der Einsatz von Kameraattrappen geplant ist. Hierbei sollte jedoch beachtet werden, dass weiterhin § 6b BDSG auch für Attrappen gilt und sofern die Attrappe nicht klar erkennbar ist in der Praxis der Betriebsrat am Besten einbezogen werden sollte und nach Darlegung des Sachverhaltes auf seine Verschwiegenheit gem. § 79 BetrVG hingewiesen wird, um den Umstand nicht bekannt zu machen.
[http://ds-its.eu/videobr]

Darf der Arbeitgeber meinen Führerschein eigentlich kopieren?

Für viele Arbeitnehmer ist die Nutzung von Dienst- oder Mietfahrzeugen an der Tagesordnung. Darf jedoch der Arbeitgeber den Führerschein aus Nachweisgründen kopieren?

(WK) Wenn ein Arbeitgeber es zulässt, dass sein Arbeitnehmer ein Firmenfahrzeug fährt, obwohl dieser nicht über die erforderliche Fahrerlaubnis verfügt, riskiert der Arbeitgeber eine Freiheitsstrafe bis zu einem Jahr. Das ergibt sich aus § 21 Abs. 1 Nr. 2 Straßenverkehrsgesetz (StVG). Außerdem droht in einem solchen Fall bei Unfällen erheblicher Ärger vor allem mit der Teil- oder Vollkaskoversicherung. In aller Regel wird die Versicherung nämlich jede Leistung verweigern. Es ist daher verständlich, dass Arbeitgeber sich gegen ein solches Risiko absichern wollen.

Zulässigkeit von Maßnahmen

Dabei wird jeodch oft gestritten, welche Maßnahmen zulässig und angemessen sind. Reicht es aus, dass der Arbeitgeber oder eine von ihm beauftragte Person (zum Beispiel ein Fuhrparkmanager) sich den Führerschein des Arbeitnehmers vorlegen lässt und eine kurze Prüfnotiz darüber anfertigt, dass die erforderliche Fahrerlaubnis vorhanden war? Oder ist der Arbeitgeber berechtigt, den Führerschein des Mitarbeiters zu kopieren und diese Kopie über einen längeren Zeitraum aufzubewahren?

Das Bayerische Landesamt für Datenschutzaufsicht als Aufsichtsbehörde für den Datenschutz in der Privatwirtschaft

hat dazu klar Stellung bezogen: Der Arbeitgeber darf in solchen Fällen den Führerschein kopieren! Eine solche Kopie sei – so das Hauptargument des Landesamts für Datenschutz – für den Arbeitgeber hilfreich, wenn er nachweisen müsse, dass die notwendige Fahrerlaubnis vorhanden gewesen sei.

Kopie zulässig

Datenschutzrechtliche Bedenken sieht das Landesamt nicht. Die Anfertigung einer Kopie ist nach seiner Auffassung für die Durchführung des Beschäftigungsverhältnisses erforderlich. Die Voraussetzungen des insoweit einschlägigen § 32 Abs. 1 Satz 1 des BDSG, der den Datenschutz im Beschäftigungsverhältnis regelt, seien daher gegeben. Der Arbeitgeber dürfe eine Kopie des Führerscheins anfertigen und aufbewahren.

Kritikern dieser Auffassung entgegnet das Landesamt, dass ein Führerschein lediglich Daten enthalte, die dem Arbeitgeber ohnehin schon bekannt seien (etwa Name und Vorname) oder die als eher banal einzustufenden Führerscheinklassen.

Kopie des Personalausweises

Hingegen ist die Anfertigung einer Personalausweiskopie regelmäßig unzulässig.

Hierzu unsere Kopiermaske: [http://ds-its.eu/pamaske]

audatis Services

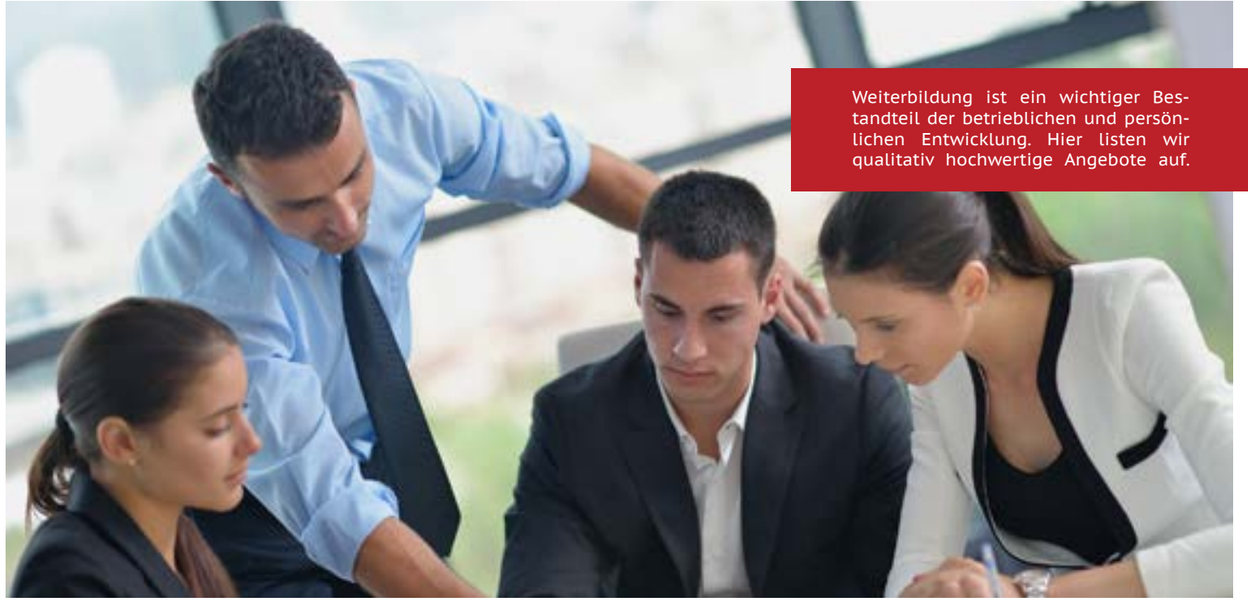
Wir stellen Ihnen diverse Arbeitshilfen, Checklisten und Software für Ihre tägliche Arbeit als Datenschutzbeauftragter online wie offline zur Verfügung.

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 November 2015 - März 2016

Ausgewählte Seminare und Webinare zu den Themen Datenschutz und Datensicherheit von November 2015 bis März 2016 im gesamten Bundesgebiet.

Termin	Veranstaltungsbeschreibung	Ort / Uhrzeit / Shortlink
17.11.	Webinar: Aktuelles im Datenschutz [Vertiefung] (audatis Training)	Online, 09:00 - 16:00 Uhr (2x2 Std.) [wbdsa]
18.11.	Webinar: Sicherheit von Content-Managm.-Syst. (CMS) (audatis Training)	Online, 10:00 - 16:00 Uhr (2x2 Std.) [wbcms]
30.11. bis 02.12.	Ausbildung zum betrieblichen Datenschutzbeauftragten (AKADEMIE HERKERT)	Frankfurt a.M. , 10:00 - 17:00 Uhr [semdsb]
12.01. bis 14.01.	Ausbildung zum betrieblichen Datenschutzbeauftragten (AKADEMIE HERKERT)	Hamburg, 10:00 - 17:00 Uhr [semdsb]
02.02.	Webinar: Aktuelles im Datenschutz [Vertiefung] (audatis Training)	Online, 09:00 - 16:00 Uhr (2x2 Std.) [wbdsa]
03.02.	Seminar: Web-Security für Web-Entwickler (audatis Training)	Köln, 09:00 - 17:00 Uhr [wswe]
09.02.	Seminar: Datenschutz für IT-Leiter und IT-Experten (audatis Training)	Köln, 09:00 - 17:00 Uhr [dsitl]
16.02.	Webinar: IT-Sicherheit für Datenschutzbeauftragte [Einstieg] (audatis Training)	Online, 10:00 - 16:00 Uhr (2x2 Std.) [wbitsds]
16.02. bis 18.02.	Ausbildung zum betrieblichen Datenschutzbeauftragten (AKADEMIE HERKERT)	Stuttgart, 10:00 - 17:00 Uhr [semdsb]
01.03. bis 03.03.	Ausbildung zum betrieblichen Datenschutzbeauftragten (AKADEMIE HERKERT)	Köln, 10:00 - 17:00 Uhr [semdsb]

Nächstes Mal

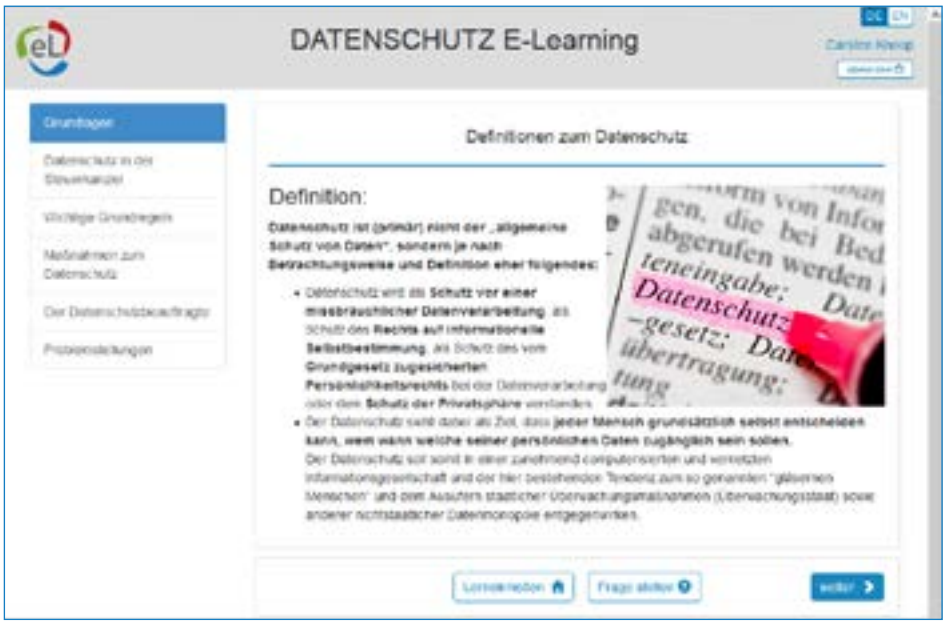
Die nächste Ausgabe des audatis.INFO Newsletters für Datenschutz und Informationssicherheit erscheint Anfang Q1 / 2016.

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

E-Learning zur Mitarbeiterschulung



(CK) In vielen Organisationen steht die regelmäßige Datenschutzschulung der Mitarbeiter auf dem Programm. Doch in vielen Fällen lässt sich nur ein Bruchteil der Belegschaft wirklich schulen. Oftmals sind es betriebliche Erfordernisse wie Schichtarbeit, zahlreiche Standorte oder Geschäftsreisende, welche eine zentrale Präsenzschulung fast unmöglich machen. Krankheiten und andere Abwesenheitsgründe von Mitarbeitern bei den angesetzten Schulungsterminen kommen erschwerend hinzu.

Ein Plan B ist dann erforderlich, um die Verpflichtungen zur Unterweisung der Arbeitnehmer mit dem Datenschutz sicherzustellen. Eine Möglichkeit ist natürlich die Zusendung oder Aushändigung von schriftlichen Unterlagen.

Viel effektiver und flexibler in der Handhabung sind jedoch E-Learnings, welche vom Mitarbeiter jederzeit an jedem Ort durchgeführt werden können.

Wir haben für einige Branchen (z.B. Steuerberater, Krankenhaus, Industrie) bereits fertige Module zur Basisschulung als E-Learning erstellt, welche mit Videos, Text und Grafiken aufbereitet sind. Abschließend kann ein Test durchgeführt werden und der Mitarbeiter erhält ein Teilnahmezertifikat als Nachweis.

Demoversionen können Sie über info@audatis.de **kostenfrei** anfordern.

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)

Erscheinungsweise
4 x jährlich

Haftung und Nachdruck
Die inhaltliche Richtigkeit und Fehlerfreiheit wird ausdrücklich nicht zugesichert. Jeglicher Nachdruck, auch auszugsweise, ist nur mit ausdrücklicher Genehmigung der Redaktion gestattet.

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