



Teil 1: Die Datenschutz-Grundverordnung und ihre Dokumentationspflichten

(CK) Ab 25. Mai 2018 gilt ein neues Datenschutzrecht in ganz Europa, das ist sicher. Jedoch sind viele Unternehmen und Datenschutzbeauftragte sehr verunsichert, was die neuen Spielregeln eigentlich für Sie konkret bedeuten und welche Herausforderungen in der „Übergangszeit“ auf sie warten oder wie sie diese bewältigen sollen.

Alleine schon die Betrachtung des Regelungsumfangs ist erdrückend. Zu den 99 Artikeln der EU Datenschutz-Grundverordnung (EU DS-GVO) gesellen sich noch 173 Erwägungsgründe, welche ausdrücklich zum Gesetz dazu gehören und entsprechend beachtet werden müssen. Hinzu kommen noch nationale Datenschutzregeln in Form von weiteren Datenschutzgesetzen (in Deutschland einem neuen BDSG), welche die Grundverordnung ergänzen sowie natürlich weiteren Gesetze mit Rechtsgrundlagen für die Verarbeitung personenbezogener Daten (wie gehabt) z.B. TMG, SGB und andere. Da fällt es trotz der „Vereinheitlichung“ des Datenschutzes noch schwerer den Überblick zu behalten.

Erhöhte Dokumentationspflichten

Eine zentrale Änderung durch die DS-GVO wird für alle Unternehmen jedoch mit Sicherheit die Einführung der „Rechenschaftspflicht“ sein, welche gem. Art. 5 Abs. 2 DS-GVO von den Verantwortlichen fordert, dass sie „die Einhaltung des Gesetzes nachweisen können“. Das hört sich zunächst nicht so dramatisch an, bei rechtlicher Betrachtung folgt daraus jedoch, dass es nicht mehr wie bisher nach BDSG ausreicht, sich an das Gesetz bei der Verarbeitung zu halten und die Aufsichtsbehörden einem erst einen Verstoß nachweisen müssen, um ein Bußgeld zu verhängen. Die Lage ist ab 2018 umgedreht: Sie müssen jederzeit in der Lage sein die Rechtmäßigkeit nachweisen zu können. D.h. schon alleine der fehlende Nachweis (in der Regelfall also die notwendige Dokumentation) kann zu einem Bußgeld führen, selbst wenn die dazugehörige Verarbeitung der Daten rechtskonform erfolgt.

Erhöhte Bußgelder

Da gerade das Stichwort Bußgeld gefallen ist, soll natürlich auch nicht unerwähnt bleiben, dass dieses von den bisher im BDSG bekannten Höhen von

IN DIESER AUSGABE

- Dokumentationspflichten1
- Verfahrensverzeichnis2
- Aktuelles Recht & Technik...3
- Sichere Apps? Der Test3
- Mitarbeiterschulung4
- Veranstaltungen4
- Löschkonzept5
- Coaching / Impressum6

EDITORIAL

Liebe Leser,

Die EU Datenschutz-Grundverordnung wirft derzeit bei vielen Unternehmen und Datenschützern Fragen auf, die wir in unserem Newsletter in den nächsten Ausgaben zu beantworten versuchen. Dabei haben wir uns für das Motto: „weniger ist mehr“ entschieden und unseren Newsletter vom Umfang reduziert, um Ihnen häufiger Informationen zukommen lassen zu können, als das in den letzten Monaten der Fall war.



Carsten Knopf

Fortsetzung des Artikels von Seite 1 ...

50.000 bzw. 300.000 € nun deutlich nach oben angepasst wurde. Bereits „einfache“ Verstöße können ein Bußgeld bis zu 10.000.000 € oder 2% des weltweiten Umsatzes nach sich ziehen, bei schwerwiegenderen Verstößen würden 20.000.000 € oder 4% des Umsatzes den Rahmen markieren. Damit verändert sich natürlich auch die Lage jedes Risikomanagements, denn in vielen Fällen wurden die Bußgelder als „maximaler Schadenswert“ herangezogen, da Imageschäden etc. recht schlecht zu bewerten sind und gerade im Risikomanagement von Unternehmen gerne mit „harten Fakten“ gearbeitet wird.

Dabei sollte man natürlich nicht außer

Die ominöse 250 Mitarbeiter-Regel

Angeblich soll man erst ab 250 Mitarbeitern dazu verpflichtet sein, solch ein Verzeichnis zu führen. Schaut man sich das neue Gesetz jedoch einmal genau an, so findet man in Artikel 30 DS-GVO tatsächlich eine Ausnahme. Blöderweise ist das aber in „EU-Rechtsdeutsch“ verfasst und besagt ins Deutsche übersetzt folgendes:

Eine Pflicht zur Führung des Verzeichnisses der Verarbeitungstätigkeiten besteht grundsätzlich für alle Verantwortlichen und entfällt nur, wenn jedes der folgenden Kriterien erfüllt ist:

sich natürlich jeder Geschäftsführer, der das in weiser Voraussicht bereits hat erstellen lassen. Er muss dann „nur noch schnell“ die Neuerungen ergänzen, die Rechtsgrundlagen aktualisieren, eine Risikoanalyse und entsprechende Datenschutz-Folgenabschätzung durchführen lassen und ist schon wieder auf dem aktuellen Stand.

Noch mehr Dokumentation

Sie merken schon - alleine mit dem Verzeichnis ist es nicht getan. Da kommt noch mehr Arbeit auf die Unternehmen bzw. ihre Datenschutzexperten zu. Dazu aber im nächsten Newsletter (Teil 2) mehr...

“Die Ausnahme zur Führung eines Verzeichnisses der Verarbeitungstätigkeiten gilt maximal für Kaninchenzuchtvereine ohne Vereinsverwaltung und regelmäßige Veranstaltungen.“

acht lassen, dass hiermit zunächst nur ein Rahmen festgesteckt wurde und nicht grundsätzlich die finale und einzelfallbezogene Bußgeldhöhe feststeht. Das war aber auch bisher nicht der Fall. Dafür steht jedoch fest, dass bereits für Verstöße gegen die Verordnung, die bisher komplett ohne Bußgeld „verpufften“ der kleine oder große Bußgeldrahmen gezogen werden kann.

Verfahrensverzeichnis notwendig?

Dazu gehört beispielsweise die bisher unter dem Begriff „Verfahrensverzeichnis“ bei Unternehmen doch recht ungeliebte und vernachlässigte Dokumentation aller automatisierten Verarbeitungsvorgänge. Die brauchte man zwar offiziell auch schon bisher gem. § 4g Abs. 2 BDSG jedoch gab es kein direktes Bußgeld bei Nachlässigkeiten in diesem Bereich. Zukünftig kann das im Bereich bis zu 10 Mio. € liegen, wenn man die nun als „Verzeichnis von Verarbeitungstätigkeiten“ bezeichnete Dokumentation nicht vorlegen kann. Immerhin muss diese trotz gestiegener Transparenz-anforderungen nicht mehr öffentlich gemacht werden. Doch sicherlich haben Sie schon von einer Ausnahme dieser Regel gehört?!

- **Es werden weniger als 250 Mitarbeiter beschäftigt UND**
- **die Verarbeitung birgt keine Risiken für die Rechte und Freiheiten der Betroffenen UND**
- **die Verarbeitung erfolgt nur gelegentlich UND**
- **es werden keine besonderen Datenkategorien gem. Art. 9 Abs. 1 DS-GVO und Art. 10 DS-GVO verarbeitet.**

Damit fällt einem versierten Datenschützer dann vermutlich auch kein Beispiel mehr ein, für welches diese Ausnahme überhaupt gelten kann. Vielleicht für den „Verein der Kaninchenzüchter“, welcher lediglich „gelegentlich“ zu einer Versammlung einlädt (auf keinen Fall „regelmäßig“) und seine Mitgliedsliste (mit Daten aus dem öffentlichen Telefonbuch) noch in einem unter Verschluss gehaltenen Vereinsbuch führt. Jede regelmäßige Gehaltsabrechnung im Unternehmen torpediert diese Ausnahme dann auch schon im 3-Mitarbeiter-Betrieb.

Somit müssen sich nun alle Unternehmen mit dem Verzeichnis der Verarbeitungstätigkeiten beschäftigen und dieses entsprechend der gesetzlichen Vorgaben dokumentieren. Hier freut

Wie muss das neue Verzeichnis aussehen und wie geht man vor?

Wir haben hier einmal exemplarisch die Beschreibung einer Verarbeitungstätigkeit dokumentiert, welche im Laufe der nächsten Newsletter um weitere Inhalte ergänzt werden, damit Sie das Verzeichnis als zentrale Dokumentationsstelle verwenden können.

Wer bisher schon ein Verfahrensverzeichnis auf Basis der Angaben des BDSG erstellt hat, kann dieses erweitern (die in *blau und kursiv* dargestellten Inhalte sind somit „*alt-Lasten*“ und werden um die anderen Angaben ergänzt).

Beispiel eines Bewerberverfahrens zur externen Stellenbesetzung

- a) *Mustermann GmbH, Musterstr. 12, 12345 Musterstadt*, Tel. 0123-456789, info@mustermann.de, *Geschäftsführer: Peter Muster*, Datenschutzbeauftragter: Carsten Knoop.
- b) *Zweck der Verarbeitung ist die Durchführung von Bewerberauswahlverfahren auf externe Stellenausschreibungen.*
- c) *Beschreibung der betroffenen Personen: Externe Bewerber deren Datenkategorien: Namen,*

Kontaktdaten, Lebenslauf, Anschreiben, Zeugnisse, Foto

- d) *Kategorien von Empfängern: Personalabteilung, Betriebsrat, Geschäftsführung, Vorgesetzte der jeweiligen suchenden Fachabteilung, externer Dienstleister (Bewerbungsplattform X)*
- e) *Keine Datenübermittlung ins Drittland*
- f) *Löschung der kompletten Bewerbungsdaten nach 6 Monaten, beginnend mit dem Tag der Absage*
- g) *Beschreibung der allg. Maßnahmen TOM*

Es wäre natürlich schön, wenn Sie damit schon fertig wären, denn die Neuerungen halten sich ja in Grenzen. Doch die DS-GVO fordert weit mehr, es müssen nämlich zukünftig bei jeder Erhebung von personenbezogenen Daten dem Betroffenen weitere Informationen mitgeteilt werden, damit eine gem. Art. 13 DS-GVO „faire und transparente“ Datenverarbeitung gewährleistet werden kann.

Zentrale Sammelstelle

Wo wenn nicht im Verzeichnis der Verarbeitungstätigkeiten würden diese Informationen besser gesammelt und zentral dokumentiert?

Daher hier unser Vorschlag auf Erweiterung des Verzeichnisses um folgende Informationen für den Betroffenen:

- h) Rechtsgrundlage für die Datenverarbeitung: ist die Einwilligung des Bewerbers gem. Art. 7 DS-GVO.
- i) Der Verantwortliche beabsichtigt diese Daten nicht für andere Zwecke zu verwenden.
- j) Herkunft: Die Daten wurden direkt beim Betroffenen erhoben.

Noch lange nicht fertig...

Damit haben Sie schon einmal eine gute Grundlage, um mit der Verzeichniserstellung zu beginnen oder das vorhandene zu überarbeiten. Jedoch ist die Dokumentation damit noch nicht erledigt und wir werden in der nächsten Ausgabe weitere Pflichten und Ergänzungen beleuchten.

Für Sie gefunden: Aktuelles aus Datenschutz und Technik

EU-U.S. Privacy-Shield aktiv

Da es seit dem 01.08.2016 für U.S.-Unternehmen möglich ist, sich nach den Regeln des EU-U.S. Privacy Shield zu zertifizieren, finden sich auf der vom U.S. Handelsministerium geführten Liste bereits eine Anzahl von Unternehmen, für die der Selbst-Zertifizierungsprozess abgeschlossen ist. Da der Beschluss der Europäischen Kommission zum Privacy Shield bindend ist, kann das Privacy Shield nun trotz der von den Datenschutzbehörden geäußerten Kritik an den Regelungen als Grundlage genutzt werden, um personenbezogene Daten aus Europa an zertifizierte U.S.-Unternehmen zu transferieren. Die für den Datenexport verantwortlichen europäischen Stellen haben dabei stets darauf zu achten, dass das U.S.-Unternehmen, an das die Daten übermittelt werden, auch tatsächlich auf o.g. Liste des U.S.-Handelsministeriums eingetragen ist. Ferner muss das datenexportierende Unternehmen anhand des Listeneintrags auch überprüfen, ob die Zertifizierung auch die Kategorie von Daten umfasst (Beschäftigtendaten="HR" oder sonstige Daten = "Non HR"), die übermittelt werden sollen.

<http://ds-its.eu/euuslst>

Der von der Europäischen Kommission zum Privacy Shield veröffentlichte Leitfaden für Bürger und Bürgerinnen, in dem vor allem die Rechte Betroffener dargestellt werden, ist inzwischen auch in deutscher Sprache verfügbar.

<http://ds-its.eu/euusps>

EuGH entscheidet über IP-Adressen

Nach jahrelangem Rechtsstreit fällt der EuGH am 19.10.2016 endlich das Urteil zum Umgang mit dynamischen IP-Adressen für Webseitenbetreiber.

Der EuGH stimmte dem Kläger zu, dass die dynamische IP-Adresse als personenbezogenes Datum gelte, sofern der Webseitenbetreiber „über rechtliche Mittel verfügt, die es ihm

erlauben, den Nutzer anhand der Zusatzinformationen, über die dessen Internetzugangsanbieter verfügt, bestimmen zu lassen.“ Gleichzeitig urteilte das Gericht, dass der Betreiber einer Webseite aber ein berechtigtes Interesse daran haben kann, bestimmte personenbezogene Daten der Nutzer zu speichern, um sich gegen Cyberattacken verteidigen zu können.

<http://ds-its.eu/jureuip>

BSI Entscheidungshilfe für Manager

Am 02.12.16 veröffentlichte das BSI eine Broschüre, die Entscheidern aus Wirtschaft und Verwaltung einen ersten Einblick zur Bedeutung eines ganzheitlichen Managementsystems für Informationssicherheit (ISMS) ermöglicht. Die bewährte IT-Grundschutz-Methodik stellt ein differenziertes Angebot bereit, das passgenaue Lösungen für individuelle Sicherheitsanforderungen einer Institution liefert.

<http://ds-its.eu/bsimb>

Windows 10 und Arbeitnehmer?!

Der freizügige Umgang von Windows 10 mit den Daten seiner Nutzer könnte nicht nur datenschutzrechtlich problematisch sein, sondern auch gegen deutsche Arbeitnehmerrechte verstoßen. Wie iX in seiner aktuellen Ausgabe 11/2016 berichtet, übermittelt das Betriebssystem persönliche Daten etwa zur Softwareinstallation, die Adressen der vom Webbrowser Edge aufgerufenen Webseiten, Suchanfragen an Bing und sogar die Klickpfade der Office-Software an Microsoft. In Büros laufe das auf eine Überwachung der Arbeitnehmer hinaus, was nach gängiger Rechtsauffassung nicht zulässig ist. Das Bayerische Landesamt für Datenschutzaufsicht untersucht derzeit, ob ein datenschutzkonformer Einsatz von Windows 10 überhaupt möglich ist.

<http://ds-its.eu/win10ds>

Datenschutzschulung für Ihre Mitarbeiter

Datenschutz kann als Wettbewerbs- und Marketingvorteil genutzt werden, um das Vertrauen von Kunden und Für viele Datenschutzbeauftragte ist die Motivierung der Mitarbeiter zur Umsetzung der Datenschutzvorschriften eine Sisyphe-Aufgabe und wird als Arbeitsbehinderung, etc. abgetan. Noch schlimmer ist die Situation, wenn sogar die Führungskräfte nicht von der Notwendigkeit des Datenschutzes und der entsprechenden Einhaltung im Unternehmen überzeugt sind dann fehlt den Mitarbeitern das Vorbild und sie werden sich erst recht nicht an die Datenschutzanforderungen halten.

audatis hat die Probleme der Datenschutzbeauftragten, aber auch die Argumente der Mitarbeiter und Manager, analysiert und daraus ein Datenschutz-Schulungskonzept zur Sensibilisierung von Mitarbeitern im Unternehmen entwickelt (Datenschutz-Awareness). Dieses enthält:

- Abstimmung der Inhalte mit dem betrieblichen DSB
- Erstellung der Schulungsunterlagen (PDF + PPT)
- Schulung durch unsere Referenten bei Ihnen vor Ort (ca. 1,5 Std. / Gruppe)
- Integration von Live-Hackings und Beispielen aus Betrieb und Privatem

Bei Interesse oder Fragen:

training@audatis.de

Veranstaltungen und Seminare Dezember 2016 bis März 2017

Im **Bereich Datenschutz** finden folgende Veranstaltungen zwischen **Dezember 2016 und März 2017** statt, die wir Ihnen empfehlen können:

Termin	Veranstaltungsbeschreibung	Ort / Uhrzeit
07.12.	Webinar: Aktuelles im Datenschutz [Vertiefung] in 2 x 2 Stunden	Online, 9:00 - 16:00 [wbdsa]
14.03. bis 16.03.	Ausbildung zum betrieblichen Datenschutzbeauftragten (AKADEMIE HERKERT)	Stuttgart, 10:00 - 17:00 [semdb]
23.03.	Webinar: Aktuelles im Datenschutz [Vertiefung] in 2 x 2 Stunden	Online, 9:00 - 16:00 [wbdsa]
27.03. bis 30.03.	Datenschutzauditor (TÜV Rheinland Akademie)	München, 9:00 - 17:00 [tuvdsa]
28.03.	Webinar: Datenschutz für IT-Leitern und IT-Experten in 2 x 2 Stunden	Online, 9:00 - 16:00 [dsitl]
29.03. bis 30.03.	Datenschutz in medizinischen Einrichtungen (TÜV Rheinland Akademie)	Köln, 9:00 - 17:00 [tuvmed]
28.03. bis 30.03.	Ausbildung zum betrieblichen Datenschutzbeauftragten (AKADEMIE HERKERT)	Frankfurt, 10:00 - 17:00 [semdb]

Der audatis Shortlink

Sie finden weitere Informationen zu den Veranstaltungen und die jeweiligen Veranstalter oder zu weiterführenden Informationen und Downloads 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.



Die DVD-Spezialschulung für Datenschutz in der Zahnarztpraxis

Carsten Knoop stand in diesem Jahr für die i-med Akademie vor der Kamera und hat einen Teil seiner Erfahrungen zum Thema „Datenschutz in der Zahnarztpraxis“ in Form einer Lern-DVD weitergegeben. Erfahren Sie in 3 x 45 Minuten, wie eine optimale Umsetzung von Datenschutz und Datensicherheit entsprechend dem Bundesdatenschutzgesetz (BDSG) in Ihrer Zahnarztpraxis erfolgen kann und sichern Sie sich dazu noch 6 CME Fortbildungspunkte.



Sie erhalten die DVD samt den 10 Checklisten und Formularen derzeit über unseren Online-Shop für nur 145 EUR inkl. Online-Lerntest zur Beantragung der CME Punkte.

<http://ds-its.eu/dvdds>

Personenbezogene Daten gesetzeskonform Löschen

(RK) Das Bundesdatenschutzgesetz und auch die europäische Datenschutz Grundverordnung fordern, dass personenbezogene Daten gelöscht werden, sobald der Zweck, für den sie erhoben wurden, erfüllt ist oder nicht mehr besteht. Ausnahmen bestehen da, wo weitere Gesetze eine Aufbewahrungspflicht enthalten.

Nachweis der Löschung

Die Löschung muss im Zweifelsfall entweder dem Betroffenen oder der Aufsichtsbehörde nachgewiesen werden können. Dem Nachweis dient das Löschkonzept zusammen mit den Löschkonzepten. Doch was verbirgt sich dahinter eigentlich?

Aufbewahrungsfristen gelten.

Personenbezogene Daten, die in die externe Auftragsdatenverarbeitung (ADV) gehen, sind ebenso zu berücksichtigen, wie die Daten, die Sie zur Auftragsdatenverarbeitung von Kunden erhalten. Im Falle der ADV muss zwischen Auftragnehmer und Auftraggeber eine angemessene Frist zur Löschung vertraglich vereinbart werden.

Ableitung von Löschrregeln

Aus den gesammelten Datenarten, Nutzungszeiträumen und Aufbewahrungsfristen können die Löschrregeln abgeleitet werden. Spätestens an

Konzepte ist, dass Daten nicht ohne Dokumentation bewegt, gesperrt oder gelöscht werden. Es sollte bei jedem dieser Vorgänge ein Protokoll entstehen, dass abgelegt wird, damit die Löschrungen / Sperrungen / Archivierungen sauber belegt werden können.

Sonderfall externer Datenträger

Externe Datenträger können als Sonderfall betrachtet werden, insbesondere, wenn sie zum Datentransfer außer Haus genutzt werden. Sehen Sie für diese Datenträger eine schnellstmögliche Löschung vor, nachdem die Daten sicher in das Zielsystem überführt sind. Für be-

“Daten dürfen nicht ohne Dokumentation bewegt, gesperrt oder gelöscht werden. Daher sind Löschrprotokolle besonders wichtig.“

Im Datenschutzrecht gilt der Grundsatz, dass so wenig personenbezogene Daten wie möglich so kurz wie nötig vorgehalten werden sollen (§ 3a BDSG, Art. 5 Lit. c DS-GVO). Ein Löschkonzept sollte also vorsehen, alle personenbezogenen Daten im Unternehmen so schnell wie möglich zu löschen. Des Weiteren muss es zusätzlich vorsehen, dass ein Betroffener jederzeit der Speicherung von Daten widersprechen kann (Art. 21 DS-GVO), und seine personenbezogenen Daten, bis auf die Teile, die rechtlichen Vorhaltefristen unterliegen, zeitnah gelöscht werden müssen. Diese Vorgaben werden bei einem Löschkonzept nach DIN 66398 berücksichtigt. Daher geht auch dieser Vorschlag nach der DIN-Norm vor.

Aller Anfang ist schwer

Zu Anfang des Löschkonzepts steht die Erfassung aller Arten von personenbezogenen Daten, die im Unternehmen erhoben, verarbeitet und genutzt werden. Hier sollte auf das bereits eingangs im Newsletter erwähnte Verzeichnis (Seite 2-3) zurückgegriffen werden. Gleichzeitig wird festgehalten, wie lange ein Datensatz zur Bearbeitung benötigt wird, unter welchen Umständen er noch einmal zu anderen Zwecken gebraucht wird, und ob gesetzliche

diesem Punkt sollte die IT-Abteilung hinzugezogen werden, um zu überprüfen, wie eine datenschutzkonforme Löschung mit der im Betrieb genutzten Software machbar ist.

Die Löschrregeln sind das zentrale Dokument des Löschkonzepts. Aus diesem ergeben sich die weiteren Dokumente, die nach Abteilungen und Datenarten gegliedert sind.

Legen Sie auch mit der IT-Abteilung und den bearbeitenden Abteilungen fest, ob und wie Dateien aus dem Produktivsystem nach der Bearbeitung in die Archivierung überführt werden. Beachten Sie bei der Archivierung auch die Löschrfristen. Eine saubere und konsequente Löschung der Daten nach den Aufbewahrungsfristen ist um so einfacher, wenn ein Archiv (Datei oder Datenträger) nur gleich lang aufzubewahrende und im gleichen Lauf zu löschende Daten enthält. Diese Archivierungskonzepte kann die Abteilung auch selbständig mit der EDV aufstellen, sie müssen allerdings dann vom Datenschutzbeauftragten geprüft werden.

Gleiches gilt für Löschrungen, die unmittelbar aus dem Produktivsystem erfolgen.

Nachvollziehbarkeit

Die wichtigste Anforderung an alle

sonders sensitive Daten empfiehlt sich dann auch eine physische Zerstörung des Datenträgers.

Alle Störungen von Löschr-, Sperr- oder Archivierungsläufen müssen gesondert behandelt werden, auch dafür ist es sinnvoll in einem Dokument niederzulegen, wer in einem solchen Fall Ansprechpartner ist, und wo eine Fehlermeldung aufläuft.

Selbstverständlich müssen alle betreffenden Dokumente angepasst werden, wenn neue Verfahren eingeführt werden, zu speichernde Datenarten oder IT-Systeme geändert werden.

Die Aufteilung des Löschkonzepts in verschiedene Dokumente ermöglicht dabei eine flexible und einfache Anpassung der einzelnen Teile.

Eine kurze Anleitung „in 8 Schritten zum datenschutzkonformen Löschkonzept“ können Sie sich über folgenden Shortlink herunterladen:

<http://ds-its.eu/dsdel>

Unsere Leistung

Wir bieten Beratung bei der Erstellung von Löschkonzepten und Löschrprotokollen.

Datenschutz-Coaching 2017

Unsere Online-Services für Sie

Nutzen Sie unsere kostenlosen Checklisten und Muster zur einfachen und schnellen Umsetzung des Datenschutzes in Ihrem Unternehmen. Im Bereich Ratergeber / Business stehen Ihnen diese zum Download bereit:

<http://ds-its.eu/ratbus>

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>

(JB) Die ersten Unternehmen haben sich schon monatelang mit der neuen Rechtslage auf Basis der EU Datenschutz-Grundverordnung beschäftigt und ihre Datenschützer auf zahlreiche Seminare geschickt.

Was ist aber mit all den Unternehmen, Selbständigen, Vereinen und Verbänden, die sich das bisher nicht leisten konnten oder wollten?

Hier wird niemand eine Agenda vorbereiten, welche Schritte bis Mai 2018 umzusetzen sind, um nicht in ein dann deutlich höheres Bußgeldrisiko zu geraten. Bei der Umsetzung wird vermutlich auch niemand mithelfen, denn es hat ja niemand eine konkrete Vorstellung oder Fachkunde, was denn nun genau gemacht werden soll. Und selbst bei gut geschulten Datenschutzbeauftragten, wird es zum Ende der Übergangsfrist vermutlich recht unangenehm werden, weil

das ein oder andere Thema leider auf der Strecke geblieben ist zwischen all den Dingen, die man eben noch so „nebenbei“ erledigen muss.

Da wir all diese Szenarien bereits kennen und Ihnen hier mit unserem Wissen aus der Praxis für die Praxis gerne weiterhelfen möchten, werden wir Anfang 2017 ein Datenschutz Coaching anbieten, welches auf mehreren Säulen basierend, Sie bis zur Umsetzung eines Datenschutz-Managementsystems - je nach individuellem Bedarf - begleitet.

Dabei gehören regelmäßige Webinare und Telefonate, eine E-Mailberatung, Checklisten und eine Datenschutz-Software mit Umsetzungsanleitungen sowie integriertem E-Learning zum Leistungsumfang. Melden Sie sich bei Interesse gerne vorab: coaching@audatis.de

Hat Ihnen unser Newsletter gefallen?

Dann empfehlen Sie diesen doch weiter:

www.audatis.de/online/newsletter

Die nächste Ausgabe dürfen Sie in
Q1 / 2017 erwarten.

IM NÄCHSTEN NEWSLETTER:

DS-GVO Dokumentationspflicht (Teil 2)
Veranstaltungen + Aktuelle Themen

Impressum

audatis Consulting
Datenschutz und Informationssicherheit
Inh. Carsten Knoop

Leopoldstr. 2-8
32051 Herford

Redaktion:

V.i.S.d.P. Carsten Knoop (CK)
Jill Bohrenkämper (JB)
Regina Küpper (RK)

Erscheinungsweise: ca. 4 x jährlich

Kontaktmöglichkeiten

So können Sie uns zu allen Fragen oder Anregungen erreichen:

Telefon: 05221 85496 - 90

Telefax: 05221 85496 - 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

Haftung und Nachdruck:

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