Datenschutzaudits sind wichtig

September | 2015

Wichtige Datenschutzinformationen für Ihr Unternehmen

DPN
Datenschutz &
Informationssicherheit

Inhalte | Datenschutzinformationen | September 2015

Inhaltsverzeichnis

Begrüßung | Ihr Datenschutzbeauftragter vor Ort

Fabio Pastars

Liebe Leserin, lieber Leser,

viele Vorgänge und Abläufe in Ihrem Alltag sind aus datenschutzrechtlichem Betrachtungswinkel sicher intuitiv oder auch bewusst richtig organisiert.

Wenn Sie aber als verantwortungsbewusster Unternehmer oder Bereichsleiter auf die Einhaltung des Datenschutzes in Ihrem Unternehmen gezielt hinwirken möchten, kommen Sie an einem fundierten und strukturierten Datenschutzaudit nicht vorbei.

Es ist die einzige Chance zu erkennen, ob und wie Sie schon im Sinne des Gesetzes handeln und – noch wichtiger – was in Ihrem Unternehmen noch fehlt, um von einer gesetzeskonformen Verarbeitung von personenbezogenen Daten sprechen zu können.

Es ist im Datenschutz nicht anders als in anderen Bereichen. Ohne IST-Wert ist das Setzen von Zielen schwierig, der anschließende Vergleich der Ergebnisse und der Veränderungen sogar unmöglich.

Wir haben Ihnen mit dieser Ausgabe unserer Broschüre umfassende Informationen über Datenschutzaudits zusammengefasst, um Ihnen einen verständlichen Überblick darüber zu geben und Ihnen ans Herz zu legen, sich damit auseinander zu setzen.

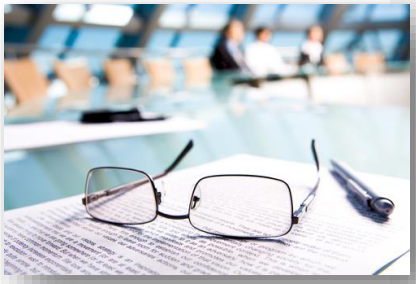
Fokussieren Sie im Audit das, was Ihnen für Ihr Unternehmen, Ihre Mitarbeiter und für Ihre Kunden wichtig erscheint. Sie werden erkennen, welche Vorteile sich für Sie und Ihr Unternehmen langfristig ergeben.

Sollten Sie darüber hinaus weitere Informationen benötigen oder eine ausführliche Beratung in Anspruch nehmen wollen, stehen wir Ihnen jederzeit sehr gerne zur Verfügung. Sie erreichen uns unter der Telefonnummer + 49 (2163) 341 371 - 0 oder per E-Mail an info@dpn-datenschutz.de.

Mit besten Grüßen

Fabio Pastars

Externer Datenschutzbeauftragter (nach DIN EN ISO/IEC 17024)
Consultant für Datenschutz und Informationssicherheit



Sinn und Zweck eines Datenschutzaudits

Jedes privatwirtschaftliche Unternehmen in Deutschland ist zum Datenschutz verpflichtet und hat dabei die Vorgaben des Bundesdatenschutzgesetzes sowie anderer Rechtsvorschriften zu beachten und umzusetzen. Wie genau dies erfolgen soll und wie ein Datenschutzbeauftragter vorzugehen hat, ist nicht konkret definiert.

Um festzustellen, wo ein Unternehmen steht und wie weit die Umsetzung der gesetzlichen Vorgaben fortgeschritten ist, bietet sich die Durchführung eines Datenschutzaudits an. Ein Datenschutzaudit folgt einer festgelegten Struktur und Vorgehensweise.

Ziel eines solchen Audits ist also die Ermittlung des bestehenden Datenschutzniveaus im Unternehmen. Erst durch den Abgleich der IST-Situation mit den gesetzlichen Anforderungen wird es möglich, den Handlungsbedarf zu erkennen und konkrete Handlungsempfehlungen und Optimierungsvorschläge zu formulieren.

Ein Datenschutzaudit sollte durch unabhängige Experten, z.B. Datenschutz-auditoren oder externe Datenschutzbeauftragte, durchgeführt werden. Besonders für interne Datenschutzbeauftragte ist dies sehr hilfreich, da durch das Datenschutzaudit und die resultierenden Handlungsempfehlungen ihre bisher geleistete Arbeit überprüft und kommentiert wird.

Oftmals finden sich in den Handlungsempfehlungen Aufgaben oder Bereiche, die der interne Datenschutzbeauftragte zuvor ebenfalls schon thematisiert hatte und die von der Geschäftsleitung aber ignoriert oder abgelehnt wurden.

Datenschutzaudit – Was soll auditiert werden?

Zielsetzung

Vorab ist es wichtig, das Ziel des Datenschutzaudits klar zu definieren. Die Geschäftsleitung des Unternehmens muss festlegen, was genau auditiert werden soll. Dies wird als Zielsetzung festgehalten und vereinbart. Es stehen verschiedene Arten von Audits zur Auswahl, die Einfluss auf die jeweilige Durchführung haben.

Allgemeines Datenschutzaudit

Ziel des allgemeinen Datenschutzaudits ist es, das aktuelle Datenschutzniveau zu ermitteln und die Konformität zu den gesetzlichen Vorgaben zu prüfen. Lässt ein Unternehmen zum ersten Mal ein Audit durchführen, wird in der Regel diese Form durchgeführt.

Einzelaudits

Hierbei werden einzelne Bereiche auditiert. Das können einzelne Anwendungen sein, wie z.B. ERP-Systeme oder Anwendungen zur Zeiterfassung oder Personalverwaltung. Aber auch Prozesse, wie z.B. das Kundenmanagement, können herangezogen werden.

Zertifizierungsaudit

Solche Audits haben zum Ziel gewisse Standards zu prüfen, die für den Erhalt bestimmter Zertifizierungen erforderlich sind, wie z.B. ISO oder BSI.

Technische Audits

Bei technischen Audits wird der Fokus meist auf die IT-Sicherheit im Allgemeinen oder sogar nur auf einzelne Systeme oder Anwendungen gerichtet. Ziel kann z.B. die Sicherheit einer Serverfarm im Rechenzentrum oder der Schutz von personenbezogenen Daten bei der Übermittlung sein.

Organisatorische Audits

Die Prüfung von organisatorischen Maßnahmen ist hier Grundlage des Audits. Dazu zählen z.B. Managementsysteme zur Informationssicherheit oder auch Qualitätsmanagement-Handbücher, sofern sie für die Verarbeitung von personenbezogenen Daten relevant sind. Oder auch die Einhaltung der Vorgaben der Auftragsdatenverarbeitung nach § 11 BDSG kann ein mögliches Ziel sein.

Datenschutzaudit – Reporting und weiteres Vorgehen

Analyse und Ergebnis

Nach Durchführung des Audits werden alle Informationen ausgewertet und in Relation zu den gesetzlichen Vorgaben bzw. zu den definierten Zielen gesetzt.

Hieraus erfolgt die Erstellung eines Auditberichts für das Unternehmen. Der Bericht enthält eine Zusammenfassung des Auditziels und eine Beschreibung der Vorgehensweise bei der Durchführung. Daran angeschlossen folgt eine detaillierte Erklärung in Bezug auf die Zielerreichung und ggf. Abweichungen.

Maßnahmenliste / Handlungsempfehlungen

Die Liste der Maßnahmen bzw. Handlungsempfehlungen darf natürlich nicht fehlen, denn sie ist Grundlage für das weitere Vorgehen des Unternehmens.

Sie sollte folgende Gliederung aufweisen:

- ✓ Getroffene Feststellung, also welche Ausgangssituation der Auditor vorgefunden hat.
- ✓ Resultierende Maßnahme. Was genau ist zu tun, um die Abweichung abzustellen.
- ✓ Rechtsvorschrift. Diese begründet die empfohlene Maßnahme.
- ✓ Umsetzungsgrad. Eventuell befindet sich die Maßnahme bereits in der Umsetzungsphase.
- ✓ Risikobewertung. Realistische Einschätzung des Risikos bei Nichtumsetzung der Maßnahme.
- ✓ Potentielle Sanktionen. Welche möglichen Strafen oder Bußgelder kommen auf die Geschäftsleitung zu, wenn eine Umsetzung der Maßnahme abgelehnt wird.

Die Umsetzung der Maßnahmen ist nicht Teil des Audits und muss vom Unternehmen selbst verantwortet werden. In der Regel wird dies an den internen bzw. externen Datenschutzbeauftragten delegiert.

Das IT-Sicherheitsgesetz ist am 25.07.2015 in Kraft getreten

Aktuelle Fragen und Antworten zum neuen Gesetz für IT-Sicherheit

Für wen gilt das Gesetz?

Betreiber von Webangeboten (z.B. Online-Shops). Für sie gelten nun erhöhte Anforderungen an die technischen und organisatorischen Maßnahmen zum Schutz ihrer Kundendaten und der von ihnen genutzten IT-Systeme.

Telekommunikationsunternehmen. Sie sind verpflichtet, ihre Kunden zu warnen, wenn sie bemerken, dass sein Anschluss für IT-Angriffe (z.B. Spamversand) genutzt wird. Gleichzeitig sollen sie Wege zur Beseitigung der Störung aufzeigen.

Betreiber Kritischer Infrastrukturen (KRITIS). Sie werden verpflichtet, die IT-Systeme, die für die Erbringung ihrer wichtigen Dienste erforderlich sind, nach dem Stand der Technik angemessen abzusichern. Eine Überprüfung der Angemessenheit muss alle zwei Jahre erfolgen. Darüber hinaus müssen die Betreiber dem BSI erhebliche IT-Sicherheitsvorfälle melden. Die Meldepflicht betrifft zunächst nur Kernkraftwerke und Telekommunikationsunternehmen, eine Meldepflicht für andere KRITIS-Betreiber tritt erst nach Verabschiedung der noch zu erstellenden Rechtsverordnung in Kraft. Dann erst wird klar sein, welche Unternehmen noch dazu zählen.

Was müssen Webseitenbetreiber nun beachten?

Webseitenbetreiber müssen angemessene Maßnahmen ergreifen, um unbefugte Zugriffe auf ihre Systeme und Daten zu verhindern. Sie müssen auch durch entsprechende Maßnahmen dafür sorgen, dass Störungen vermieden werden.

Was bedeutet Stand der Technik?

In der Gesetzgebung wird dieser Begriff genutzt, weil die technische Entwicklung deutlich schneller ist als die Anpassung der Gesetze erfolgen könnte. Was zu einem bestimmten Zeitpunkt Stand der Technik ist, lässt sich anhand existierender Standards wie DIN oder ISO oder anderer praxisnaher Referenzen ermitteln. Da sich die erforderlichen Maßnahmen meist je nach konkreter Situation unterscheiden, ist eine allgemeingültige Definition nicht möglich.

Datenschutzbeauftragter und Betriebsrat

Schnittstellen

Aufgabe des Betriebsrats ist es unter anderem, die freie Entfaltung der Persönlichkeitsrechte der Beschäftigten zu schützen und zu fördern (§ 75 Abs. 2 BetrVG). Dabei hat der Betriebsrat alle Gesetze, Tarifverträge und Vereinbarungen zu überwachen, die in irgendeiner Form zum Schutz von Arbeitnehmern vorgesehen sind.

Der Datenschutzbeauftragte hat auf die Einhaltung des Datenschutzes hinzuwirken und die Betroffenenrechte der Mitarbeiter zu schützen. Dabei ist er auf solche Gesetze beschränkt, die den Datenschutz betreffen.

In manchen Bereichen wird es regelmäßig Überschneidungen geben, bei denen beide Parteien involviert sein werden. Insbesondere dann, wenn es um die Erstellung und den Abschluss von Betriebsvereinbarungen geht.

Da ist es hilfreich, wenn ein gutes Klima unter den Parteien herrscht und eine partnerschaftliche Zusammenarbeit möglich ist.

Zuständigkeit und Verantwortung

Grundsätzlich verantwortet die Geschäftsleitung eines Unternehmens die Einhaltung des Datenschutzes. Ist ein Datenschutzbeauftragter bestellt, ist es seine primäre Aufgabe, auf die Einhaltung des Datenschutzes hinzuwirken. Dabei obliegen dem Datenschutzbeauftragten gewisse Kontrollrechte im gesamten Unternehmen. Diese erstrecken sich jedoch nicht auf den Betriebsrat.

Der Betriebsrat ist für die Einhaltung des Datenschutzes selbst verantwortlich und darf nicht durch den Datenschutzbeauftragten kontrolliert werden. Er darf sich aber natürlich freiwillig von ihm unterstützen lassen.

Dies ist auch ratsam, da im Betriebsrat oft besonders sensible personenbezogene Daten verarbeitet werden.

Datenschutzbeauftragter und Betriebsrat

Restrisiko für die Geschäftsleitung

Der Betriebsrat verarbeitet teilweise sensible Mitarbeiterdaten.

Der Geschäftsführer hat einen Datenschutzbeauftragten bestellt, dieser darf den Betriebsrat aber nicht kontrollieren, ebenso wenig die Geschäftsleitung.

Der Betriebsrat ist aber Teil der verantwortlichen Stelle, also steht die Geschäftsleitung auch in der Haftung.

Die Geschäftsleitung muss also sicherstellen, dass mit dem Betriebsrat ein Teil des Unternehmens, zu dem niemand über Kontrollrechte verfügt, die gesetzlichen Vorgaben zum Datenschutz einhält.

Eine anspruchsvolle Aufgabe, die einen vertrauensvollen Umgang zwischen allen Parteien erfordert.

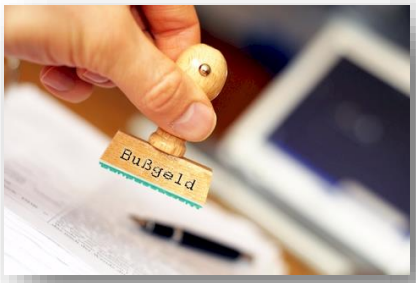
Mitbestimmung des Betriebsrats bei der Bestellung eines DSB?

Häufig hört oder liest man, dass Betriebsräte der Meinung sind, bei der Bestellung des Datenschutzbeauftragten ihr Mitbestimmungsrecht nach § 87 BetrVG geltend machen zu können.

An dieser Stelle sei gesagt, dass sich das Mitbestimmungsrecht ausdrücklich nicht darauf erstreckt. Höchstens dann, wenn die Bestellung eines internen Datenschutzbeauftragten auch andere Personalmaßnahmen nach sich zieht, die wiederum eine Mitbestimmung durch den Betriebsrat begründen.

Bestellt die Geschäftsleitung einen externen Datenschutzbeauftragten, ist eine Beteiligung des Betriebsrates an dem Entscheidungsprozess ausgeschlossen.

Auftragsdatenverarbeitung - Bußgeld durch die Aufsichtsbehörde



BayLDA setzt Bußgeld in fünfstelliger Höhe fest

Wer einen externen Dienstleister als einen so genannten Auftragsdatenverarbeiter mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beauftragt, muss mit diesem gemäß § 11 BDSG einen schriftlichen Vertrag abschließen.

Das Gesetz schreibt insgesamt zehn Regelungsbereiche vor, die zum Schutz der personenbezogenen Daten vertraglich festgelegt werden müssen. Von besonderer Bedeutung sind dabei die technischen und organisatorischen Maßnahmen (Anlage 1 zu § 9 Satz 1 BDSG), die der Auftragnehmer zum Schutz der Daten treffen muss.

Der Auftraggeber bleibt für die Daten verantwortlich, daher ist es seine Pflicht, dafür zu sorgen, dass diese Maßnahmen konkret festgelegt und schriftlich dokumentiert werden. Unterlässt er dies oder ist die Beschreibung nicht konkret genug, stellt dies eine Ordnungswidrigkeit dar, die mit Geldbuße von bis zu 50.000,- € geahndet werden kann.

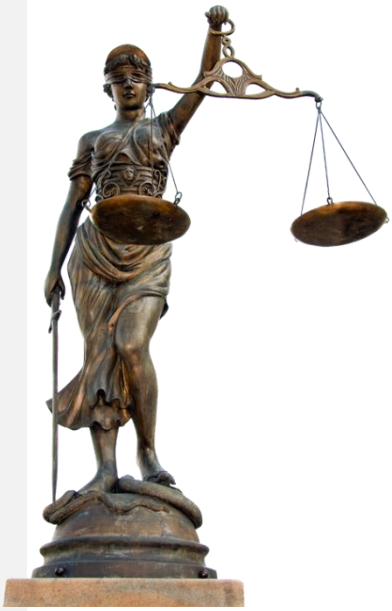
Das BayLDA hat kürzlich gegen ein Unternehmen eine Geldbuße in fünfstelliger Höhe festgesetzt. Das betroffene Unternehmen lässt Daten im Auftrag verarbeiten. Es hatte in seinen schriftlichen Vereinbarungen mit mehreren Auftragnehmern jedoch keine konkreten technischen und organisatorischen Maßnahmen zum Schutz der Daten festgelegt. Die Vereinbarungen enthielten nur einige pauschale Aussagen und Wiederholungen des Gesetzestextes.

Das Bayrische Landesamt für Datenschutzaufsicht hat festgestellt, dass dies keinesfalls ausreicht. Als Auftraggeber muss das Unternehmen beurteilen können, ob der Auftragnehmer im Rahmen der Verarbeitung für die Sicherheit der Daten sorgen kann. Diese Beurteilung kann mangels ausführlicher Beschreibung nicht sicher getroffen werden. Auch muss der Auftraggeber die Einhaltung der technischen und organisatorischen Maßnahmen bei seinem Auftragnehmer kontrollieren. Wie sollen jedoch eine Kontrolle und eine Beurteilung möglich sein, wenn die entsprechenden Maßnahmen nicht klar definiert sind?

FAZIT

Die korrekte Durchführung von Datenverarbeitung im Auftrag muss zur Pflicht für jedes Unternehmen werden. Sind die internen Abläufe einmal klar definiert, dann ist der Aufwand in Relation zur Sicherheit der Daten und zur Erreichung der Gesetzeskonformität angemessen und vertretbar.

Datenschutzvorfälle



Massenhaft Kundendaten an falschen Empfänger gesendet

Ein o2-Kunde aus Kiel bekommt seit mehr als einem Jahr regelmäßig E-Mails, die für andere Kunden des Unternehmens bestimmt waren – inzwischen mehr als 600 Daten wie Kontonummern, Adressen, Geburtsdaten, eingescannte Unterschriften und Ausweisnummern landeten so fälschlicherweise bei dem Kieler. Die sensiblen Daten stammen von Berliner o2-Kunden, die ihren Vertrag in einem der dortigen o2-Shops abgeschlossen haben. Die kurze Mailadresse des Kieler Kunden wurde dort "offenbar zuweilen als Dummy bei neuen Handyverträgen eingegeben", heißt es im Bericht von shz.de.

Quelle: shz.de vom 02.09.2015

Festplatte mit Schülerdaten auf Trödelmarkt gekauft

Auf einem Trödelmarkt in Köln hatte ein Bürger aus Frechen eine gebrauchte Festplatte erstanden. Als er sie zu Hause anschloss, entdeckte er Zeugnisse, Gutachten und Klassenfotos von Grundschülern einer Stadt aus dem Nachbarkreis. Auf dem Datenträger war etwa ein Bericht über den sonderpädagogischen Förderbedarf eines Schülers zu finden. Namen, Adresse und Telefonnummer der Eltern des Schülers erfuhr man ebenso. Die Dokumente seien dem Bericht zufolge allein mit einem Windows-Passwort geschützt und leicht mit einem Linux-Betriebssystem zu umgehen gewesen. Wie sich herausstellte, stammt die Festplatte aus dem Rechner eines Mannes, der ihn zum Sperrmüll an die Straße gestellt hatte, ohne die Daten seiner Frau, einer Grundschullehrerin, zu löschen.

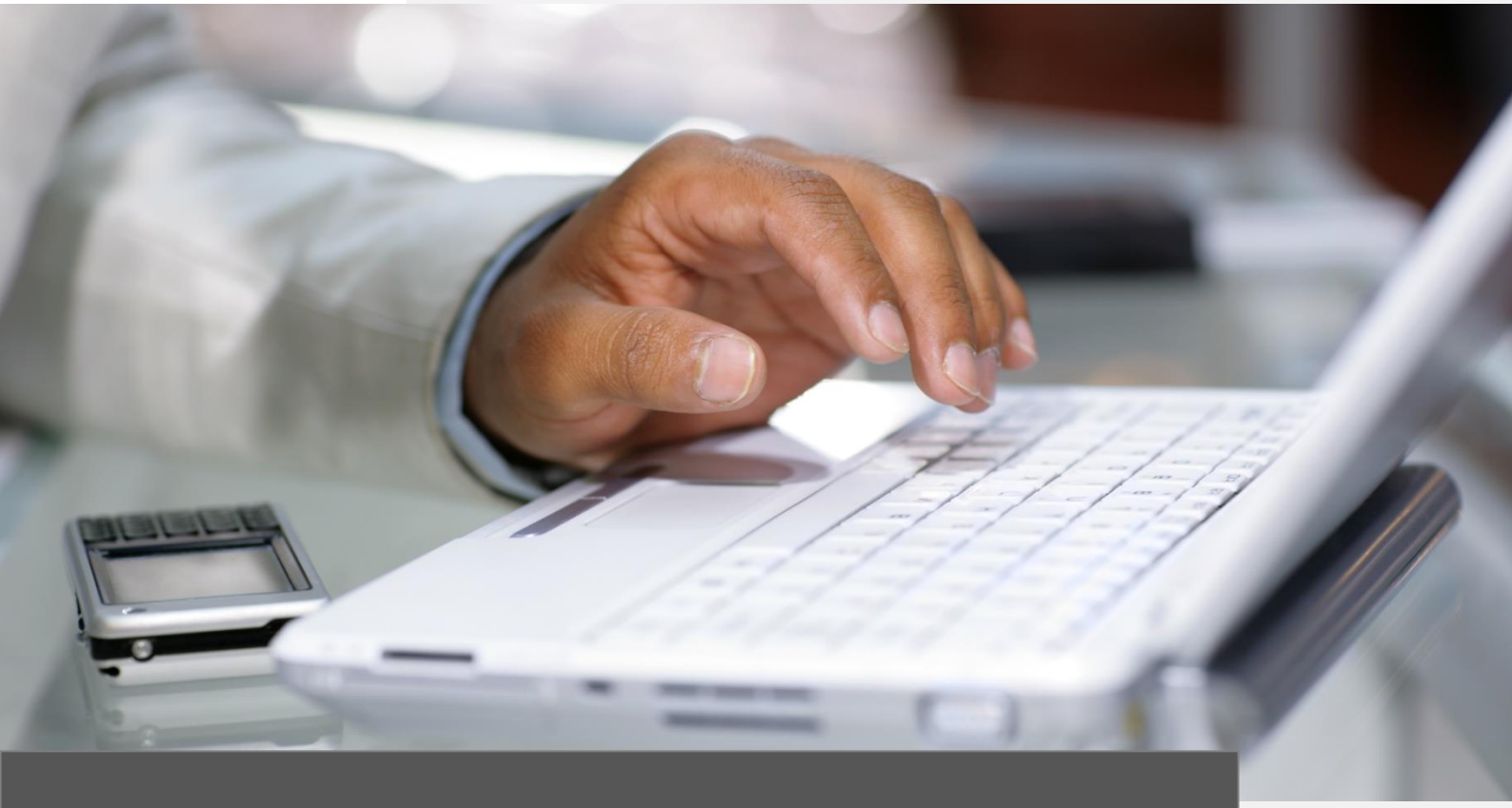
Quelle: Rhein-Erft Rundschau online vom 05.08.2015

Urlaubsplanung öffentlich einsehbar

Die Urlaubsplanung von Mitarbeitern der Tropenklinik Paul-Lechler-Krankenhaus stand für jeden abrufbar im Internet, da das Intranet der Klinik nicht geschützt war. In einer Tabelle waren Urlaubszeiten von 30 mit Namen genannten Mitarbeitern für 2013 bis 2015 in einer Tabelle festgehalten. Es war auch nachzulesen, wann jemand keinen Bereitschaftsdienst machen kann und wann jemand Nachtdienst machen möchte. Bei einer Mitarbeiterin konnte man sehen, wann sie wieviel Fehltage wegen Krankheit hatte.

Quelle: heise.de vom 05.06.2015

September | 2015



Impressum

DPN Datenschutz GmbH & Co. KG
Hochstraße 2
41379 Brüggen
Tel.: +49 (2163) 341 371 - 0
Fax: +49 (2163) 341 371 - 9
Web: www.dpn-datenschutz.de
E-Mail: info@dpn-datenschutz.de

Amtsgericht Krefeld, HRA 6213
Ust-IdNr.: DE275528415
p.h.G.: DPN Verwaltung GmbH
Geschäftsführer: Fabio Pastars
Amtsgericht Krefeld, HRB 14208

Redaktion:
Fabio Pastars

Bildnachweise:
Diese Datenschutzbroschüre wurde in unserem Auftrag von der Firma ITKservice GmbH & Co. KG, Fuchsstädter Weg 2, 97491 Aidhausen erstellt. Alle in diesem Dokument dargestellten Bilder wurden von der ITKservice GmbH & Co. KG bei der Firma ccvision.de gekauft und lizensiert.

DPN
Datenschutz & Informationssicherheit