Datenschutzvorfälle & Informationspflicht

März | 2015

Wichtige Datenschutzinformationen für Ihr Unternehmen

DPN
Datenschutz &
Informationssicherheit

Inhalte | Datenschutzinformationen | März 2015

Inhaltsverzeichnis

Begrüßung| Ihr Datenschutzbeauftragter vor Ort _____ 3

Datenschutzvorfälle & Informationspflicht | Was tun? _____ 4

Strategie und Maßnahmen zur Vermeidung von Datenschutzvorfällen _____ 7

Sensibilisierung der Mitarbeiter zu Datenschutz und IT-Sicherheit _____ 9

Aktuelle Datenschutzvorfälle in Unternehmen und öfftl. Stellen _____ 11

Begrüßung | Ihr Datenschutzbeauftragter vor Ort

Fabio Pastars

Liebe Leserin, lieber Leser,

was der Verlust von sensiblen personenbezogenen Daten oder die unbefugte Kenntnisnahme durch Dritte für Folgen haben können, lesen wir mittlerweile fast täglich in den Medien.

Immer wieder tauchen Sicherheitslücken in Onlineshops auf, Kundendaten sind aufgrund von Datenbank- oder Konfigurationsfehlern öffentlich einsehbar oder unachtsame Mitarbeiter übermitteln Daten unverschlüsselt an falsche Empfänger.

Und als ob das nicht schon genug Risiken sind, steigt auch die Anzahl der weltweiten Cyber-Attacken täglich. Dabei haben es die Angreifer durch die moderne Technik mittlerweile sehr komfortabel. Wo Taschendiebe noch körperlich aktiv werden mussten, führen die modernen Kriminellen ihre Beutezüge bequem vom Sofa aus.

Auch das Ziel der Kriminellen hat sich verändert. War es früher das Bargeld, auf das sie es abgesehen hatten, geht es heute überwiegend um persönliche Informationen wie beispielsweise Daten zu Kreditkarten und Bankkonten.

Unser aller Aufgabe liegt nun darin, den Schutzbedarf solcher Informationen zu ermitteln und den Zugriff durch unbefugte Dritte durch individuelle Sicherheits-strategien und geeignete Maßnahmen zu verhindern.

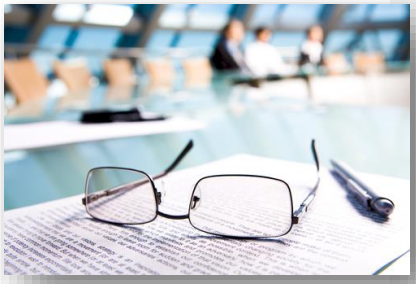
Ein optimales Datenschutz-Sicherheitsniveau herzustellen, Ihre Mitarbeiter zu sensibilisieren und möglichst alle potentiellen Fehler zu vermeiden; das sind die Ziele dieser Ausgabe. Und sollte es trotz aller Maßnahmen dennoch einmal zu einem Verstoß kommen, erläutern wir auf folgenden Seiten, was zu tun ist.

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 (DIN EN ISO/IEC 17024 zertifiziert)
Consultant für Datenschutz und Informationssicherheit



Informationspflicht nach § 42a BDSG

Wenn personenbezogene Daten, die als besonders vertraulich gelten, auf irgendeine Weise Dritten unrechtmäßig zur Kenntnis gelangen, greifen die Bestimmungen des § 42a Bundesdatenschutzgesetz.

Dazu genügen schon der Versand von vertraulichen Daten an einen falschen Empfänger, der Verlust oder Diebstahl von mobilen Geräten oder Datenträgern oder der unbefugte Zugriff auf Kundendaten durch Sicherheitslücken in Online-systemen, beispielsweise einem CRM-System oder einem Shop.

Sind solche vertraulichen Daten betroffen, muss die verantwortliche Stelle die Betroffenen und die zuständige Datenschutz-Aufsichtsbehörde direkt informieren, sofern aus einer unrechtmäßigen Kenntnisnahme von Daten für den Betroffenen schwerwiegende Beeinträchtigungen seiner Rechte oder seiner schutzwürdigen Interessen entstehen können.

Die Einschätzung über die Schwere der zu erwartender Beeinträchtigungen muss die verantwortliche Stelle selbst vornehmen. In jedem Fall sollte der Datenschutzbeauftragte diesen Prozess begleiten. Es empfiehlt sich auch, den Vorgang zu dokumentieren und die getroffene Einschätzung zu argumentieren.

Folgende Datenarten fallen dabei unter die Informationspflicht

- ✓ Besondere Arten personenbezogener Daten (§3 Abs. 9 BDSG). Besonders relevant sind hier Gesundheitsdaten und Personaldaten.

- ✓ Personenbezogene Daten, die einem Berufsgeheimnis unterliegen (§ 203 StGB). Dies betrifft Steuerberater, Anwälte, Notare, Ärzte, aber auch z.B. Angehörige privater Kranken-, Unfall- und Lebensversicherungen.

- ✓ Personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht auf solche beziehen. Zum Beispiel Ordnungswidrigkeiten, die mit einem Firmenfahrzeug begangen wurden oder Beschäftigtendaten, die zur Aufdeckung einer Straftat erhoben wurden.

- ✓ Personenbezogene Daten zu Bank-und Kreditkartenkonten. Hierzu zählen Kontonummern, Transaktionsdaten, Bankbelege, Kontoauszüge etc.

Benachrichtigung an den Betroffenen

Der Betroffene ist unverzüglich zu informieren, sobald angemessene Maßnahmen zur Wiederherstellung der Sicherheit der Daten ergriffen sind. Das Schließen der Sicherheitslücke hat dabei Vorrang.

Wenn durch die Benachrichtigung etwaige Ermittlungen von Strafverfolgungsbehörden gefährdet werden könnten, muss die Benachrichtigung unterbleiben. Und zwar so lange, bis eine Gefährdung der Strafverfolgung ausgeschlossen werden kann.

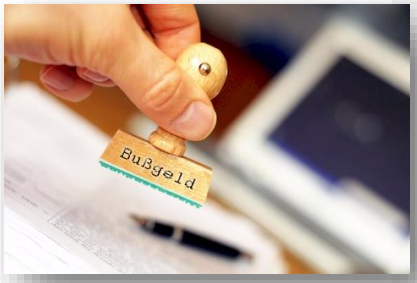
Inhalte der Benachrichtigung

Die Benachrichtigung muss den Betroffenen über die Art der Datenpanne und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen in Kenntnis setzen. Dazu gehört auch die explizite Nennung der betroffenen Daten, damit der Betroffene sich der möglichen Risiken bewusst wird und konkrete Maßnahmen einleiten kann.

Form der Benachrichtigung

Grundsätzlich ist jeder Betroffene einzeln zu benachrichtigen. Die verantwortliche Stelle sollte den Nachweis der Benachrichtigung erbringen können. Welche Form dafür angemessen sein kann, hängt von den ihr zur Verfügung stehenden Daten ab. In den meisten Fällen wird die verantwortliche Stelle die Betroffenen per Briefpost benachrichtigen. Denkbar wäre auch der Versand per Einschreiben, um im Falle eines Schadensersatzverfahrens den Erhalt der Benachrichtigung nachweisen zu können.

Bei einem unverhältnismäßig hohen Benachrichtigungsaufwand oder wenn die verantwortliche Stelle die Betroffenen nicht genau bestimmen kann, bleibt ihr als Alternative nur die Information der Öffentlichkeit. Das bedeutet eine mindestens halbseitige Veröffentlichung in mindestens zwei bundesweit erscheinenden Tageszeitungen.



Benachrichtigung an die Aufsichtsbehörde

Die Benachrichtigung der Aufsichtsbehörde muss unverzüglich erfolgen, sobald die verantwortliche Stelle Kenntnis über die Datenpanne erhalten hat. Dies sollte aus Gründen der Nachweisbarkeit immer auf schriftlichem Wege erfolgen. Eine telefonische Benachrichtigung sollte immer schriftlich nachgereicht werden.

Die verantwortliche Stelle muss der Aufsichtsbehörde zusätzlich zu den Informationen an den Betroffenen folgende Sachverhalte mitteilen:

- ✓ Zeitpunkt der Datenpanne selbst und die Feststellung darüber,
- ✓ Betroffene Daten und Art der unrechtmäßigen Übermittlung oder Kenntnisnahme,
- ✓ Darlegung möglicher nachteiliger Folgen für den Betroffenen,
- ✓ Konkrete Darlegung der ergriffenen oder geplanten Maßnahmen zur Wiederherstellung der Sicherheit der Daten und der Vermeidung für die Zukunft,
- ✓ Status der Benachrichtigung der Betroffenen.

Sanktionen

Im Falle einer nicht richtigen, nicht rechtzeitigen oder nicht vollständigen Benachrichtigung der Betroffenen oder der Aufsichtsbehörde, gleich ob aufgrund von Fahrlässigkeit oder vorsätzlich, kann die Aufsichtsbehörde dies mit einem Bußgeld von bis zu 300.000 Euro belegen.

Strategie und Maßnahmen zur Vermeidung von Datenpannen

Sinnvolle Maßnahmen zur Vermeidung von Datenpannen

Für die verantwortliche Stelle ist die Kenntnis über die Informationspflicht und die korrekte Vorgehensweise im Falle einer Datenpanne sehr wichtig. Wichtiger noch ist aber die Einleitung und Durchführung von Maßnahmen und Entwicklung von Strategien, um das Risiko von Datenpannen schon im Vorfeld deutlich zu reduzieren (Data-Loss-Prevention).

Es gibt unzählige Maßnahmen - sowohl technische als auch organisatorische -, mit denen man das Risiko sicherlich auf ein Minimum reduzieren kann. Welche davon aber für das jeweilige Unternehmen Sinn machen und umsetzbar sind, muss immer im Einzelfall betrachtet werden. Hierzu bedarf es in der Regel einer individuellen Risikoanalyse mit Fokus auf die schützenswerten Daten.

Die Informationssicherheit sollte immer als ganzheitliche Strategie verfolgt werden und nicht als Ansammlung von Einzelmaßnahmen. Als Ziel für die Umsetzung der eigenen Sicherheitsstrategie können verschiedene Referenzen herangezogen werden. Für manche Unternehmen reicht schon die Umsetzung der Maßnahmen der IT-Grundschutz-Kataloge des BSI, andere wiederum streben die Erreichung der ISO 27001 Standards an.

Nachfolgend finden Sie einige Beispiele für sinnvolle technische und organisatorische Maßnahmen:

- ✓ Identifizierung der verarbeiteten Datenarten, Schutzeinstufung der personenbezogenen Daten und Ermittlung der Schutzbedarfsklasse,
- ✓ Nachvollziehbare Berechtigungskonzepte – Mitarbeiter dürfen nur Zugriff auf für ihre Aufgaben relevante Daten haben,
- ✓ Verschlüsselung mobiler Geräte und Datenspeicher, sowie Erhöhung des Zugriffsschutzes für solche Geräte,
- ✓ Verschlüsselung der elektronischen Kommunikation, insbesondere bei der Übermittlung personenbezogener Daten,
- ✓ Unterbindung jeglicher nicht benötigter Download- und Kopierfunktionen,

- ✓ Begrenzung der Datenspeicherung auf sichere Umgebungen, Sperrung nicht benötigter USB-Schnittstellen,
- ✓ Einführung einer Password Policy,
- ✓ Umsetzung der technischen und organisatorischen Maßnahmen aus der Anlage zu § 9 BDSG,
- ✓ Regelmäßige Kontrolle der Mitarbeiter, die mit personenbezogenen Daten umgehen,
- ✓ Wiederkehrende Sensibilisierung der Mitarbeiter im Umgang mit personenbezogenen Daten,
- ✓ Auswahl externer Dienstleister ausschließlich nach den Anforderungen des § 11 BDSG,
- ✓ Anwendung der Prinzipien von Datenvermeidung (Datensparsamkeit),
- ✓ möglichst frühzeitige Anonymisierung von Daten, sobald der Personenbezug verzichtbar ist,
- ✓ Verbindliche Regelungen für die Mitarbeiter im Umgang mit der Unternehmens-IT.

Die Mindeststandards der IT-Grundschutz-Kataloge sollten in jedem Unternehmen, gleich welcher Größe, das Mindestziel der Sicherheitsstrategie darstellen.

INFO zum Bundesamt für Sicherheit (BSI)

Das Bundesamt für Sicherheit in der Informationstechnik ist eine nationale Sicherheitsbehörde. Ihr Ziel ist es, die IT-Sicherheit in Deutschland voran zu bringen. Das BSI stellt zahlreiche Werkzeuge zur Verfügung, um ein angemessenes Sicherheitsniveau zu erreichen, wie zum Beispiel die BSI-Standards zum Informationssicherheitsmanagement und die IT-Grundschutz-Kataloge.

Sensibilisierung der Mitarbeiter zu Datenschutz und IT-Sicherheit

Alle Mitarbeiter sind in der Verantwortung

Das BDSG verlangt die Umsetzung von technischen und organisatorischen Maßnahmen gemäß Anlage zu § 9 BDSG. Diese dienen der Sicherstellung der Vertraulichkeit personenbezogener Daten.

Die Ermittlung der Notwendigkeit und die Umsetzung der technischen Maßnahmen obliegen der Geschäftsführung, die diese Aufgaben jedoch in der Regel durch den IT-Verantwortlichen erledigt wissen möchte. Die gängigsten Maßnahmen wie Berechtigungs- und Datensicherungskonzepte, Password Policy, Firewalls usw. finden hier meist Anwendung. Einmal eingerichtet, greifen die technischen Regularien in der Regel zuverlässig und automatisiert. Eine vernünftige Dokumentation und regelmäßige Kontrollen sichern die Aufrechthaltung dieser Maßnahmen.

Häufig sind ungeschulte Mitarbeiter die Ursache für Datenpannen

Nicht weniger wichtig ist jedoch auch die Umsetzung organisatorischer Maßnahmen zur Sicherstellung des Schutzes personenbezogener Daten. Hier kommt der Faktor Mensch ins Spiel. Häufig ist bei Datenschutzvorfällen zu beobachten, dass die eigenen Mitarbeiter diese aus Unwissenheit oder Unachtsamkeit verursachen. Seltener als vorsätzliche Handlung, was aber dennoch als potentielles Risiko einzustufen ist.

Oft mangelt es im Unternehmen an einer strategischen Sensibilisierung der Mitarbeiter in Bezug auf die Verarbeitung von personenbezogenen Daten oder andere vertraulichen Informationen. Dieser Mangel liegt oft in Unwissenheit oder Ablehnung der Geschäftsführung begründet. Die gängigsten Ausreden lauten immer wieder „Das kostet zu viel Zeit und Geld“, „Das müssen sie auch so wissen, ist doch logisch“ oder „Wie sollen wir das denn organisieren?“.

Es steckt sicherlich etwas Aufwand dahinter, hier eine gute Organisation einzuführen. Der Mehrwert steckt dabei aber im Detail. Jeder sensibilisierte Mitarbeiter hilft aktiv mit, die Risiken für Datenschutzvorfälle zu reduzieren und trägt damit automatisch zur Sicherheit im Unternehmen bei.

Eines ist aber sicher: Spätestens nachdem ein Unternehmen das erste Mal Betroffene und Aufsichtsbehörde gemäß § 42a BDSG informieren musste, wird es sich umfassende Gedanken über einen strategischen und fortlaufenden Prozess zur Sensibilisierung seiner Mitarbeiter machen.

Sensibilisierung der Mitarbeiter zu Datenschutz und IT-Sicherheit

Individuelle Sensibilisierung ist der Schlüssel

Die Sensibilisierung der Mitarbeiter will gut strukturiert sein. Es ist wenig sinnvoll, einem Mitarbeiter alle Informationen zukommen zu lassen, obwohl dieser sie für die Ausführung seiner Aufgaben nicht benötigt.

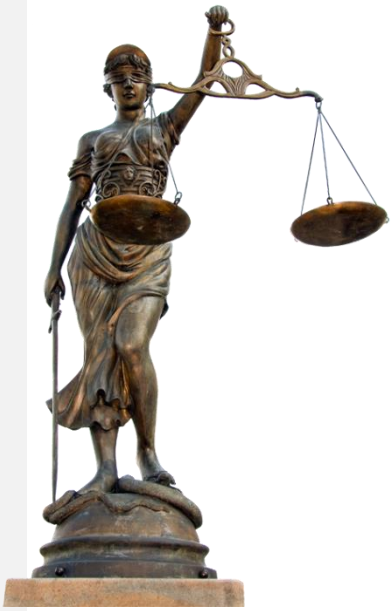
Die unnötige Informationsversorgung kostet in der Regel Zeit und damit Geld. Die Vorgaben bei der Abwicklung von Auftragsdatenverarbeitung müssen nicht für jeden einzelnen Mitarbeiter relevant sein. Besonderheiten in der Personaldatenverarbeitung betreffen in der Regel jedoch hauptsächlich Mitarbeiter dieser Abteilung.

Bei der Einführung einer Strategie zur Mitarbeitersensibilisierung sollten daher folgende Punkte Beachtung finden:

- ✓ Welche Datenkategorien verarbeitet der jeweilige Mitarbeiter? Oftmals bieten sich abteilungsbezogene Schulungen an.
- ✓ Welchem Schutzbedarf unterliegen die Daten? Dies kann den Rhythmus von Wiederholungsschulungen beeinflussen.
- ✓ Neue Mitarbeiter müssen unbedingt schon zu Beginn sensibilisiert werden.
- ✓ Regelmäßige Wiederholungs- oder Auffrischungsschulungen durchführen.
- ✓ Aufgrund reger Diskussionen sind Präsenzschulungen webbasierten Trainings möglichst vorzuziehen.
- ✓ Themenorientierte Schulungen kommen beim Teilnehmer besser an.
- ✓ Immer mit Beispielen aus der Praxis arbeiten, um das Verständnis der Teilnehmer zu fördern.
- ✓ Nicht stur Folien vortragen, sondern in den Dialog mit Mitarbeitern treten. Auch das fördert das Verständnis der Teilnehmer.

Die Schulungen zu den einzelnen Themenbereichen Datenschutz und Informationssicherheit sollten jeweils von Experten mit entsprechenden Fachwissen vermittelt werden. Aufgrund der Komplexität der Themen und der Fülle an Vorgaben sind Selbstlernprozesse weniger zu empfehlen.

Aktuelle Datenschutzvorfälle in Unternehmen und öffentlichen Stellen



Kindergeldakten in Arbeitsagentur frei zugänglich

In der Frankfurter Arbeitsagentur sind Akten mit persönlichen Daten wie Kontonummern, Verdienstbescheinigungen und Geburtsurkunden tagelang offen zugänglich gewesen. Kindergeldempfänger in Frankfurt, dem Hoch- und dem Maintaunuskreis waren davon betroffen. Eine Sprecherin der Regional-direktion bestätige dies umgehend. *(Quelle: Focus online vom 09.03.2015)*

Mangelhafter Datenschutz bei Infoscore

Infoscore ist eine der größten deutschen Auskunfteien. Der Radiosender NDR Info gibt an, dass Unbefugte sich problemlos Zugang zu den Daten von etwa acht Millionen in Zahlungsschwierigkeiten befindliche Verbraucher verschaffen konnten. Hierzu war es lediglich notwendig, auf dem Onlineportal für Mieterselbstauskünfte Name, Geburtsdatum und Anschrift einer Person anzugeben und dafür ca. 20 Euro zu bezahlen. Infoscore hat umgehend mit der vorübergehenden Deaktivierung der betroffenen Webseite reagiert. *(Quelle: Spiegel online vom 23.03.2015)*

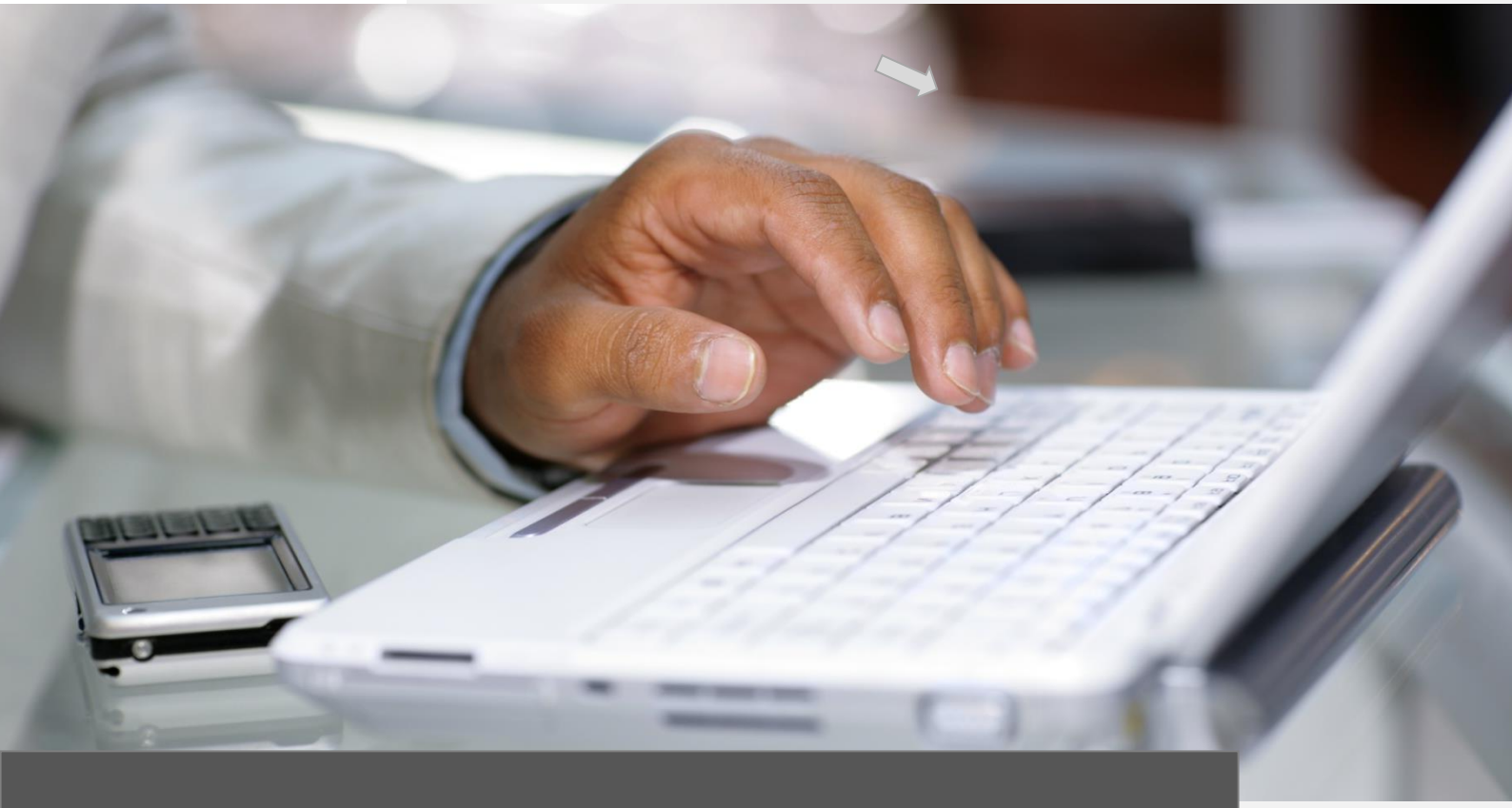
Patientenunterlagen am Straßenrand gefunden

Bei der Entsorgung alter Patientenunterlagen der Klinik Weilheim kam es zu einer Datenpanne. Von den 90 Säcken mit Röntgenbildern, die von einer Entsorgungsfirma abgeholt worden waren, fanden sich mindestens vier am Straßenrand in München-Neuperlach wieder. Auf den Bildern befanden sich die Namen und Geburtsdaten der Patienten. *(Quelle: Süddeutsche.de online vom 12.02.2015)*

Gemeinde Alpen unterläuft Datenpanne beim E-Mail Versand

106 Bewerbern sollte eine Absage per E-Mail erteilt werden. Die Gemeinde Alpen am Niederrhein hat dabei den kompletten Verteiler der Mitbewerber auf "cc" gesetzt. So war für jeden Bewerber ersichtlich, wer sich noch auf die Stelle beworben hatte. Dass es das erste online durchgeführte Ausschreibungs-verfahren war, kann nicht als Ausrede gelten. *(Quelle: RP online vom 27.11.2014)*

März | 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