Datenschutzverstöße können teuer werden!

September | 2013

Wichtige Datenschutzinformationen für Ihr Unternehmen

DPN
Datenschutz &
Informationssicherheit

Inhalte | Datenschutzinformationen | September 2013

Ihr Datenschutzbeauftragter vor Ort

Fabio Pastars

Liebe Leserin, lieber Leser,

vor kurzem wurde eine Mitarbeiterin eines bayerischen Handelsunternehmens damit beauftragt, einen größeren Teilnehmerkreis per E-Mail zu informieren. Sie schrieb den Inhalt, selektierte die Kunden, kopierte diese in die Vorlage und bestätigte die Versendung. Ein einfacher Vorgang, der täglich tausendfach vorkommt. Das Dumme hierbei war nur, dass sie die E-Mail-Adressen in das „An-Feld“ kopierte – ein folgenschwerer Fehler. Da viele Adressen aus dem Vor- und/oder Nachnamen bestehen (= personenbezogene Daten) und in diesem Fall diese durch die fehlerhafte Eingabe für alle Teilnehmer sichtbar waren, ein eindeutiger Verstoß gegen Datenschutzvorschriften.

Genau so wurde das auch vom Bayerischen Landesamt für Datenschutz gesehen, die für diesen Verstoß direkt ein Bußgeld verhängten.

An diesem kleinen Beispiel erkennen Sie, wie schnell es durch Unwissenheit oder Fahrlässigkeit zu einer Missachtung der Datenschutzgesetze kommen und erhebliche Konsequenzen für Mitarbeiter, Unternehmen und Geschäftsführung nach sich ziehen kann. Aber nicht nur die finanziellen Risiken sollten berücksichtigt werden. Es steht auch immer der Ruf des Unternehmens auf dem Spiel und somit sollte man zwingend darauf achten, alle Mitarbeiter zu sensibilisieren, wenn es um das Thema Datenschutz geht.

Um Ihnen einen kleinen Überblick zu verschaffen, wo Gefahren für Ihr Unternehmen lauern könnten, haben wir in dieser Ausgabe ein paar kleine Beispiele selektiert und zusammengestellt.

Falls Sie über diese Informationen hinaus eine ausführliche Beratung nutzen möchten, stehen wir Ihnen jederzeit sehr gerne zur Verfügung.

Sie erreichen uns unter der Telefonnummer (02153) 137 87 89 oder per E-Mail f.pastars@dpn-datenschutz.de.

Mit freundlichen Grüßen

Fabio Pastars
Zertifizierter Datenschutzbeauftragter
(Fachhochschule Südwestfalen und DEKRA)

Gesetzesgrundlagen und Datenschutzkontrollen

Die Gesetzesgrundlage

Alle Unternehmen, unabhängig von deren Größe, müssen das Bundesdatenschutzgesetz (BDSG) beachten. Firmen, die mehr als neun Mitarbeiter mit Zugriff auf personenbezogene Daten beschäftigen, sind zudem verpflichtet, einen Datenschutzbeauftragten zu bestellen.

Von wem wird die Einhaltung dieser Gesetze kontrolliert?

Fast alle privaten Unternehmen (bis auf Telekommunikation und Post) unterliegen der Aufsicht der Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich. Diese sind beim jeweiligen Landesdatenschutzbeauftragten oder bei den Landesbehörden (z. B. Innenministerium) angesiedelt.

Die Kontrollgremien sind hierbei verpflichtet, allen Meldungen nachzugehen, diese zu bewerten und wenn nötig mit einem Bußgeld zu ahnden. Seit der massiven Verschärfung der Datenschutzanforderungen im September 2009, die von allen Unternehmen deutlich mehr Transparenz in Bezug auf Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten fordern, werden zudem aktive Kontrollen durchgeführt.

Egal, ob Kleinunternehmer oder Großkonzern –
eine Prüfung kann jederzeit unangekündigt ins Haus stehen.

So werden bereits seit 2010 in allen Bundesländern stichprobenartige Prüfungen durchgeführt. Hierbei wird unter anderem abgefragt, wer als Datenschutzbeauftragter bestellt ist und seit wann, ob die Tätigkeit hauptberuflich durchführt wird, weiteres Personal zur Umsetzung der Vorgaben zur Verfügung steht und wie die nötige Fachkunde erworben wurde, bzw. kontinuierlich ausgebaut wird. Da sich die Prüfungen nicht nur auf Firmen beschränken, die gesetzlich verpflichtet, sind einen Datenschutzbeauftragten zu bestellen, trifft es auch immer wieder kleine Unternehmen. Diese müssen dann ersatzweise das Verfahrensverzeichnis gemäß §4g Abs. 2 und 2a BDSG vorlegen - eine Vorgabe der Landesbeauftragten, die immer wieder viele Firmen vor große Probleme stellt.

Haftung, Strafen und Imageschäden bei Datenschutzverstößen

Wer haftet bei Datenschutzverstößen?

Sobald personenbezogene Daten nicht rechtmäßig erhoben, verarbeitet oder genutzt werden, kann dies empfindliche Strafen nach sich ziehen und Folgen für die Verantwortlichen und das Unternehmen haben. Unternehmer sind hierbei immer für die Sicherheit ihrer Datenprozesse verantwortlich und haftbar, unter Umständen sogar mit dem Privatvermögen.

Wie hoch könnten mögliche Bußgelder sein?

Eine allgemeine Formel, nach der man das Bußgeld eines Datenschutzverstoßes berechnen könnte, gibt es nicht. Es existiert auch kein Bußgeldkatalog. Hierzu sind die Unternehmen und die zu erwartenden Schäden zu vielfältig und somit hängt die Bewertung immer von vielen individuellen Faktoren ab.

Prinzipiell spielen die gesetzlichen Vorgaben eine große Rolle. Beachtet man diese, handelt nach bestem Wissen und Gewissen und dokumentiert seine Entscheidungen, wird dies positiv berücksichtigt. Hier kommt man oft mit einer kostenneutralen Anmahnung aus. Wird aber beispielsweise bewusst *kein* Datenschutzbeauftragter bestellt oder man beachtet Vorgaben wissentlich nicht, liegt automatisch ein vorsätzlich in Kauf genommenes Verschulden vor. Hier droht sehr schnell ein Bußgeld in Höhe von bis zu 50.000,00 EUR. Bei einem aktiven Verstoß, der zudem einen wirtschaftlichen Vorteil nach sich zieht, sogar bis zu 300.000,00 EUR und mehr.

Potentieller Imageschaden

Abgesehen vom finanziellen Risiko sollte man eine weitere Komponente nicht außer Acht lassen – den guten Ruf des Unternehmens. Dieser kann aufgrund der Veröffentlichungspflicht, die eine Datenschutzmissachtung nach sich zieht, nachhaltig Schaden nehmen.

Fazit: Unabhängig davon, ob ein Datenschutzbeauftragter bestellt werden muss oder nicht, ist man auf jeden Fall verpflichtet, die Datenschutzgesetze zu beachten. Falls man dies bewusst nicht tut, setzt man sich automatisch einem hohen unternehmerischen Risiko aus, welches sich existenzgefährdend auswirken könnte. Abhilfe können hier zum Teil schon kleinere Maßnahmen schaffen, wie z.B. Mitarbeiterunterweisungen, bzw. -unterlagen, die dazu verpflichten, die Datenschutzvorgaben des Unternehmens zu beachten.

Offener E-Mailverteiler | Bußgeld gegen Mitarbeiterin verhängt!

Zum Versenden einer E-Mail benötigt man nicht viel. Eine Betreffzeile, die Information und eine E-Mail-Adresse. Falls die elektronische Post direkt mehrere Personen erreichen soll, so ist auch das ohne großen Aufwand realisierbar. Einfach alle E-Mail-Empfänger in die Empfangszeile kopieren und schon ist das Rundmailing perfekt.

Vorsicht! Hier kann ein kleiner Fehler große Auswirkungen haben!

Genau solch ein „kleiner Fehler" ist einer Mitarbeiterin eines bayerischen Handelsunternehmens unterlaufen. Sie hatte die Aufgabe, eine E-Mail an Kunden zu senden, was sie wie beauftragt getan hat. Ihr Missgeschick war nur, dass sie alle Empfänger in das „An"-Feld kopierte und so die E-Mail-Adressen für den gesamten Empfängerkreis lesbar machte. Einige Kunden waren hiervon nicht begeistert und so kam es zu Beschwerden beim Bayerischen Landesamt für Datenschutz, das nach Prüfung ein Bußgeld verhängte.

Warum kam es zu einem Bußgeld?

Bei E-Mail-Adressen, die sich aus Vornamen und Nachnamen zusammensetzen, handelt es sich um personenbezogene Daten im Sinne des Datenschutzrechts. Diese Daten dürfen nur an Dritte weitergegeben werden, wenn eine Einwilligung der einzelnen Personen vorliegt oder die Weitergabe durch eine gesetzliche Grundlage geregelt ist.

Beide Voraussetzungen lagen in diesem Fall nicht vor, was einen Datenschutzverstoß zur Folge hat. Da die Zahl der Betroffenen in diesem Fall nicht unerheblich war, die Mail umfasste 10 DIN A4 Seiten, von denen neuneinhalb aus E-Mail-Adressen bestanden, hat es das BayLDA nicht bei einer folgenlosen Ermahnung bzw. Feststellung der datenschutzrechtlichen Unzulässigkeit belassen, sondern ein Bußgeld verhängt.

Bußgeld gegen die Mitarbeiterin verhängt!

In diesem speziellen Fall wurde das Bußgeld gegen die Mitarbeiterin ausgesprochen (PM vom 28.06.13). Zeitgleich teilte das BayLDA aber mit, dass in Kürze in einem vergleichbaren Fall gegen das Unternehmen entschieden wird. Hier wurde dieser Problematik „nicht die entsprechende Bedeutung beigemessen".

Fazit: Der falsche Umgang mit E-Mail-Verteilern kann schnell zu Konsequenzen führen. Daher sollte jedes Unternehmen eine Mitarbeitersensibilisierung durchführen, um auf potentielle Fehlerquellen hinzuweisen. Nur so können Bußgelder und auch ein möglicher Imageschaden vermieden werden.

Urlaubsvertretung - Weiterleitung von E-Mails

Bevor man seinen wohlverdienten Urlaub antritt, stellt sich immer wieder die gleiche Frage. Wohin mit den ankommenden E-Mails?

Hier bieten sich verschiedene Lösungen an:

- ✓ ***Alle E-Mails bleiben für die Zeit des Urlaubs ungelesen***
  Datenschutzkonform, aber leider nicht mehr zeitgemäß. Kein Unternehmen kann es sich noch leisten, beispielsweise zwei bis drei Wochen nicht zu reagieren. Eine solche Vorgehensweise würde schnell zum Verlust bestehender Kunden führen.

- ✓ ***Man bearbeitet auch im Urlaub seine Mails selbst***
  Auch hier gibt es aus Sicht des Datenschutzes keine Einwände. Dumm ist nur, dass man so auch im Urlaub erreichbar sein müsste, was die Erholung um ein Vielfaches einschränkt.

- ✓ ***Eine automatische Antwort-Mail***
  Dies ist eine gängige und datenschutzkonforme Möglichkeit, um Kunden über die eigene Abwesenheit zu informieren und gleichzeitig einen Kollegen mit ins Spiel zu bringen. Allerdings gibt es auch einen großen Nachteil dieser Vorgehensweise – der Kunde muss nach der automatischen Antwort selbst aktiv werden, um die Anfrage beim Kollegen zu starten. Tut er das nicht, könnten sicher geglaubte Aufträge verloren gehen.

- ✓ ***Direkte Weiterleitung aller E-Mails***
  Aus unternehmerischer Sicht ist die direkte Weiterleitung aller E-Mails an einen Kollegen die beste Variante. Alle Anfragen werden direkt bearbeitet und so ist eine hohe Kundenzufriedenheit garantiert. So sinnvoll diese Vorgehensweise auch sein mag, datenschutzrechtlich ist sie meist nicht zulässig, da nicht auszuschließen ist, dass auch private E-Mails für den sich im Urlaub Befindenden eingehen. Diese dürften von seiner Urlaubsvertretung nicht gelesen und schon gar nicht gelöscht werden!

Fazit: Speziell (private) E-Mails stellen aus Sicht des Datenschutzes ein erhebliches unternehmerisches Risiko dar. Hier sollte zwingend eine Mitarbeitervereinbarung getroffen werden, die den Umgang und die Weiterleitung von privaten und geschäftlichen E-Mails klar regelt.

Tipp: Mehr zum Thema Private E-Mail-Nutzung am Arbeitsplatz:
Datenschutzzeitung, Ausgabe März 2013, Seite 7-8

Bewerbungsunterlagen und der Datenschutz

Stellen Sie sich vor, Sie würden einen oder mehrere neue Mitarbeiter(innen) suchen und hierfür eine Anzeige schalten. Die Folge wäre, dass über verschiedene Wege sehr viele Bewerbungsunterlagen mit Namen, Vornamen, Geschlecht, ja sogar Familienstand und Religionszugehörigkeit bei Ihnen eingehen würden - personenbezogene Daten, die aufgrund der Datenschutzbestimmungen einem besonderen Schutz unterliegen.

Gehen Sie mit Bewerbungsunterlagen sehr sorgsam um!

Hierzu zwei Beispiele: Im Raum Frankfurt gab es innerhalb von wenigen Tagen zwei Fälle, in denen Unternehmen im Umgang mit Bewerbungsunterlagen sehr fahrlässig waren. Im ersten Fall hatte eine Firma rund 500 vermeidlich leere Mappen bei Ebay eingestellt, die zum Teil noch Lebensläufe, Fotos und Arbeitszeugnisse enthielten. Nur wenige Tage später entdeckte ein Mainzer einen weiteren Fund in einem Altpapiercontainer: Hunderte Unterlagen und Lohnsteuerkarten lagen dort zwischen vollen Aktenordnern.

Das Bundesdatenschutzgesetz sieht bei solch groben Verfehlungen Strafen von bis zu 300.000 Euro vor!

Aber unabhängig davon, dass man solch extreme Verfehlungen im eigenen Unternehmen nicht zulässt, muss man dennoch den Zugriff Unbefugter auf Bewerbungsunterlagen verhindern. Zudem muss der Personenkreis, der die Unterlagen einsehen darf, beschränkt werden. Hier dürfen beispielsweise nur die Mitarbeiter Einsicht erhalten, die mit dem Einstellungsvorgang befasst sind.

Die Frist für Klagen von Bewerbern nach AGG beträgt zwei Monate. Daher ist eine Aufbewahrung von drei Monaten sinnvoll und statthaft.

Nach einer erfolglosen Bewerbung sollten die eingereichten Unterlagen grundsätzlich vernichtet beziehungsweise an den Bewerber zurückgegeben werden. Falls man sich gegen einen etwaigen Verstoß gegen das Benachteiligungsverbot nach dem Antidiskriminierungsgesetz (AGG) absichern will, ist es zudem gestattet, die Daten über das Bewerbungsverfahren hinaus aufzubewahren. Diese sollten dann aber unter Verschluss gehalten werden. Sollten die Unterlagen eines Kandidaten behalten werden, weil sich zu einem späteren Zeitpunkt eine neue Chance bieten könnte, muss die explizite Zustimmung des Bewerbers eingeholt werden.

Fazit: Jedes Unternehmen hat dafür zu sorgen, dass beim Bewerbungsverfahren, sowohl online als auch offline, die Anforderungen des § 9 Bundesdatenschutzgesetz (BDSG) erfüllt werden. Die Verantwortung trägt der Arbeitgeber, der die Bewerberdaten immer vertraulich zu behandeln hat und bei unsachgemäßem Umgang haftet.

Kündigung: Daten von Internetseiten löschen!

Nicht selten wird im Internet mit der Kompetenz und der langjährigen Berufserfahrung von Mitarbeitern geworben. Unabhängig davon, dass man aus Datenschutzsicht hierfür eine explizite Zustimmung der betroffenen Personen benötigt, stellt sich zudem eine wichtige Frage: Was passiert nach dem Arbeitsverhältnis, nach einer möglichen Kündigung?

Hierzu gibt es ein Urteil vom LAG: Nach Beendigung des Arbeitsverhältnisses müssen Mitarbeiterdaten von allen firmenrelevanten Internetseiten gelöscht werden, da ansonsten Persönlichkeitsrechte verletzt werden könnten.

Darf man Daten ohne Einwilligung veröffentlichen?

Hierzu ein Beispiel: Eine Anwältin wechselte die Kanzlei und verlangte von ihrem früheren Arbeitgeber die Löschung aller zu ihrer Person getätigten Veröffentlichungen. Die Anwältin meinte, „… dass potenzielle Kunden, von denen sie im Internet gesucht wird, ausschließlich auf eine Kanzlei verwiesen werden, für die sie nicht mehr tätig sei." Als die Kanzlei die Löschung des Profils in Teilen ablehnte, zog die Anwältin vor Gericht.

Daten müssen gelöscht werden!

Die Anwältin bekam vom LAG Recht und die Kanzlei wurde zur Löschung der Mitarbeiterdaten verpflichtet. Die Begründung lautete „… mit der Nutzung ihrer Daten hat der frühere Arbeitgeber ihr Persönlichkeitsrecht verletzt. Schließlich hat die Frau ihre Einwilligung in die Profil-Veröffentlichung nur für die Dauer des Arbeitsverhältnisses erteilt. Eine Zustimmung für die dauerhafte Nutzung der Daten existierte dagegen nicht. Im Übrigen stellte das Anwaltsprofil keine bloße Mitteilung dar, sondern hatte werbenden Charakter: Es sollten die fachlichen Qualifikationen der Anwältin herausgestellt und Mandanten für die Kanzlei akquiriert werden. Nach Beendigung des Arbeitsverhältnisses wurden aus der Kanzlei und der Anwältin aber Konkurrenten. Wäre die Nutzung des Profils der Juristin weiterhin zulässig, entstünden der Frau erhebliche berufliche Nachteile, da ihre potenziellen Mandanten bei der Anwaltssuche im Internet ausschließlich auf die Website der konkurrierenden Kanzlei verwiesen werden."
Hessisches Landesgericht (LAG), Urteil v. 24.01.2012, Az.: 19 SaGa 1480/11.

Fazit: Bevor man Mitarbeiterdaten veröffentlicht, muss eine Einverständniserklärung vorliegen. Existiert diese nicht, handelt es sich um einen Datenschutzverstoß! Löscht man die Daten mit dem Ausscheiden aus dem Unternehmen nicht, läuft man zudem Gefahr, Schadensersatz und ein Bußgeld zu riskieren.

Empfehlung: Erstellen Sie eine Mitarbeitervereinbarung, mit der alle Abläufe, auch die nach einem möglichen Ausscheiden, detailliert geregelt werden.

Bußgeldvorschriften bei Missachtung des Datenschutzgesetzes

Die in dieser Broschüre genannten Beispiele sind nur ein Bruchteil von möglichen Aktionen von oftmals unwissenden Mitarbeitern, die ein Bußgeld oder einen Imageschaden auch für Ihr Unternehmen nach sich ziehen könnten.

Um potentielle Risiken genauer zu benennen, schreibt das BDSG genaue Tatbestände vor, die ein Bußgeld zur Folge haben können. So ist zum Beispiel in §43 BDSG eine Geldbuße in Höhe von bis zu 300.000,00 EUR und mehr vorgesehen, wenn personenbezogene Daten, die nicht allgemein zugänglich sind, unbefugt erhoben oder verarbeitet werden. Unter Umständen kann sogar eine Freiheitsstrafe von bis zu 2 Jahren drohen.

Die Frage, welche Sanktionen Unternehmen drohen, gerade im finanziellen Bereich, beantworten §43 Bußgeldvorschriften und §44 Strafvorschriften des BDSG recht ausführlich.

Die wichtigsten Punkte dieser Vorschriften haben wir folgend für Sie zusammengefasst:

§43 Absatz 1 | Geldbußen von bis zu 50.000,00 EUR für:

- ✓ Einen Verstoß gegen die Meldepflicht.
- ✓ Die fehlende, nicht rechtzeitige oder nicht ordnungsgemäße Bestellung eines Datenschutzbeauftragten (bei entsprechender Verpflichtung durch das BDSG).
- ✓ Einen Verstoß gegen eine Anordnung der Aufsichtsbehörde.
- ✓ Die nicht erfolgte, unvollständige, verspätete oder falsche Auskunft gegenüber einem Betroffenen.
- ✓ Eine fehlende Protokollierung bei automatisierten Verfahren des Datenabrufs.
- ✓ Die fehlende Widerrufsbelehrung bei einer werblichen Ansprache.
- ✓ Einen Verstoß gegen die Zweckbindung bei übermittelten Daten.
- ✓ Einen Verstoß gegen die Dokumentationspflichten bei Datenübermittlung zu Geschäftszwecken.
- ✓ Die Aufnahme personenbezogener Daten in Verzeichnisse gegen den Willen des Betroffenen.

Bußgeldvorschriften bei Missachtung des Datenschutzgesetzes

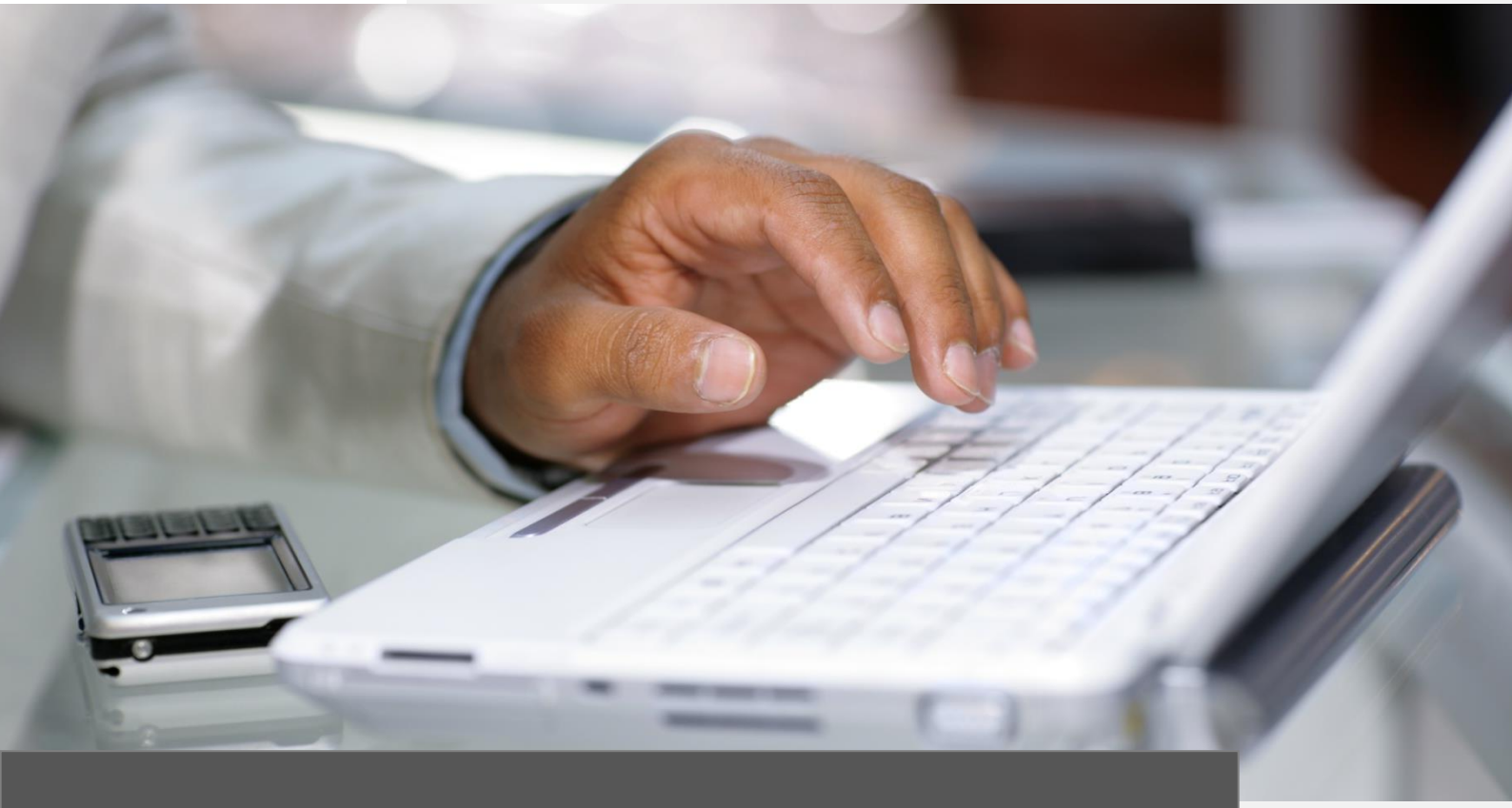
§43 Absatz 2 | Geldbußen von bis zu 300.000,00 EUR für:

- ✓ Die unbefugte Erhebung und Verarbeitung personenbezogener Daten, die nicht allgemein zugänglich sind.
- ✓ Eine unbefugte Bereithaltung personenbezogener Daten für automatisierte Abrufverfahren, die nicht allgemein zugänglich sind.
- ✓ Den unbefugten Abruf personenbezogener Daten in automatisierten Verfahren, die nicht allgemein zugänglich sind.
- ✓ Das Erschleichen einer Übermittlung personenbezogener Daten (die nicht allgemein zugänglich sind) im Abrufverfahren aufgrund unrichtiger Angaben.
- ✓ Eine Nutzung personenbezogener Daten zum Zwecke der Werbung, Markt– und Meinungsforschung, obwohl ein Widerspruch vorliegt.
- ✓ Eine nicht erfolgte, unwahre, unvollständige oder verspätete Meldung nach § 42a Satz 1 (Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten).

Denken Sie immer daran, dass Datenschutzverstöße nicht nur finanzielle Risiken mit sich führen, sondern auch den Ruf und das Ansehen des Unternehmens nachhaltig schädigen und beeinträchtigen können. Das verlorene Vertrauen zurückzugewinnen, kann unter Umständen sehr aufwändig, teuer und langwierig sein.

Zudem sollte man beachten, dass Bußgelder ja immer nur eine ergänzende Maßnahme darstellen und man aufgrund der Zahlung nicht von der Umsetzung der Datenschutzvorschriften enthoben wird. Somit entstehen – meist unter Zeitdruck – deutlich höhere Kosten, die man, beispielsweise durch eine simple Mitarbeiterbelehrung, leicht hätte vermeiden können.

September | 2013



Impressum

DPN
Datenschutz &
Informationssicherheit

DPN Datenschutz GmbH & Co. KG
Boisheimer Straße 65
41334 Nettetal
Tel.: +49 (2153) 137 87 89
Fax: +49 (2153) 137 87 84
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.