

Datenschutz Now!

Die Mitarbeiterzeitung der WEKA Business Information



Liebe Leserin, lieber Leser,

passiert eine Panne im Datenschutz, kann das nicht nur das Image des Unternehmens massiv belasten. Es drohen durchaus saftige Bußgelder, wie Sie in Ihrer neuen Mitarbeiterzeitung erfahren können. Da hilft auch kein sogenannter digitaler Radiergummi, wie er immer wieder von Politikern gefordert wird. Warum ein digitaler Radiergummi kein Datenleck ungeschehen machen kann, lesen Sie ebenfalls in dieser Ausgabe von *Datenschutz Now!*

Wie es um die ärztliche Schweigepflicht in betrieblichen Belangen steht, sollten Sie sich im Beitrag auf Seite 3 am besten sofort ansehen, genauso die Hinweise zu neuen Diensten sozialer Netzwerke wie Facebook Messages, die Ihr Datenrisiko erhöhen können. Machen Sie sich fit im Datenschutz, nicht nur für den Besuch bei Ihrem Betriebsarzt!

Für Rückfragen stehe ich Ihnen gerne zur Verfügung, Ihr *Max Mustermann, Datenschutzbeauftragter*

Facebook Messages: Der Schlüssel zu all Ihren Nachrichten

Facebook bietet mit seinem neuen Dienst Messages eine zentrale Kommunikationsplattform, mit der sich E-Mail, SMS und Chat unter einer Oberfläche vereinen lassen. Statt mehrere verschiedene Programme bedienen zu müssen, hat man bei Facebook Messages alle Nachrichten in einer Hand. Die Frage ist nur, ob es auch die eigene Hand ist ...

Facebook gewinnt weiter an Bedeutung

Mit über 500 Millionen aktiven Nutzern ist Facebook eine der führenden Online-Plattformen weltweit. Die Hälfte aller Anwender nutzt Facebook jeden Tag. Im Schnitt hat jeder Facebook-Nutzer 130 Kontakte in diesem sozialen Netzwerk. Auch Unternehmen präsentieren sich zunehmend auf Facebook, um die Beziehungen zu Interessenten, Kunden und Geschäftspartnern zu pflegen. Doch mit der Kontaktpflege und der Präsentation des eigenen Online-Profiles sind die Möglichkeiten von Facebook noch lange nicht erschöpft.

Facebook wird Kommunikationsdrehscheibe

Seit Kurzem steht den Mitgliedern von Facebook der Dienst Messages zur Verfügung. Dahinter verbirgt sich nicht einfach ein neues Angebot für kostenlose E-Mail, sondern die Bündelung von drei besonders beliebten Kommunikationsformen: SMS, E-Mail und Chat.

E-Mail oder doch SMS?

Wenn Sie Facebook Messages verwenden, müssen Sie in Zukunft nicht mehr überlegen, ob Ihnen Ihr Geschäftspartner eine SMS oder eine Mail geschickt hat, und im Internet und auf dem Handy nachsehen. Sie schauen einfach in Ihre sogenannte Social Inbox, ein Postfach, in dem auf Wunsch alle Ihre E-Mails, Chat-Nachrichten und SMS landen. Dazu muss der Absender noch nicht einmal selbst Facebookmitglied sein.

Segen oder doch Fluch?

Diese übergreifende Kommunikation scheint komfortabel und bequem. So müssen Sie sich bei Facebook Messages nur einmal mit Ihrem Passwort anmelden und nicht dauernd neue Passwörter für die verschiedenen Dienste wie Mail und Chat eintragen. Leider hat dieser Komfort einen Haken: Gelingt es einem Unbefugten, Ihr Passwort zu knacken, bekommt er nicht nur Zugang zu Ihrem Onlineprofil auf Facebook, sondern auch zu Ihren E-Mails, Chats und SMS.

Wie in Stein geritzt

Dabei könnte ein Angreifer Einblick nehmen in alle Mails, SMS und Chats, die Sie bisher über Facebook Messages geleitet haben. Denn Facebook legt ein umfassendes Nachrichtenarchiv für Sie an, das nicht etwa nach dem Abmelden von Ihrem Facebook-Konto gelöscht wird, sondern langfristig besteht.



Facebook Messages - Komfort mit Haken
(Bildquelle: facebook.com)

Mehr Dienste, mehr Einblicke

Nicht nur Dritte könnten Ihr Nachrichtenarchiv unerlaubt durchsuchen, wenn Ihr Passwort zu schwach ist. Auch böswillige Facebookmitarbeiter hätten die Chance, mehr von Ihnen zu erfahren, als es kriminellen Insidern bei einem einzelnen Mail-Anbieter oder Mobilfunk-Provider möglich wäre. Selbst wenn Facebook Ihre Daten nicht für Werbung auswertet, was von einigen Datenschützern befürchtet wird: Jede Konzentration personenbezogener Daten macht ein Angriffsziel noch interessanter. **Bevor Sie sich also für Facebook Messages oder einen anderen zentralen Kommunikationsdienst entscheiden, sollten Sie den Test auf Seite 4 machen!**

Das Internet kennt kein Verfallsdatum

Politiker wollen den Datenschutz im Internet stärken und fordern einen digitalen Radiergummi. Damit soll es möglich werden, im Internet veröffentlichte Daten endgültig zu löschen. Vertrauen Sie aber lieber nicht auf diesen Radiergummi, sondern auf Ihre Datensparsamkeit.

Im Internet verewigt

Haben Sie einmal mit einer der Internetsuchmaschinen nach Ihrem Namen gesucht? Dann waren Sie sicherlich erstaunt, wo Ihr Name und Ihre Daten überall zu finden sind. Vielleicht haben Sie sich auf einer Firmen-Webseite als Referenzkunde gefunden, obwohl Sie dem nicht zugestimmt haben. Oder Sie finden einen alten Kommentar von sich in einem Online-Forum, an den Sie sich lieber nicht erinnern wollen. Oder haben Sie einmal einen Online-Wunschzettel in einem Webshop hinterlegt und finden jetzt Ihre früheren Wünsche eher peinlich? Am besten wäre es, diese alten Daten einfach zu löschen.

Das Löschen wird gern vergessen

Um die Löschung personenbezogener Daten steht es aber nicht immer gut, insbesondere im Internet. So häufen sich die Beschwerden, dass Online-Anbieter die Konten ehemaliger Nutzer nicht rechtzeitig löschen und dass persönliche Daten, die auf einer Online-Plattform gelöscht wurden, plötzlich auf einer anderen Webseite wieder auftauchen. Manche Online-Dienste gleichen einem Elefanten mit seinem hervorragenden Gedächtnis und merken sich die Daten länger, als den Betroffenen lieb ist.



Der digitale Radiergummi ist keine Ideallösung für Daten im Internet

Wollen Sie Ihre Daten löschen?

Da ist die Forderung mancher Politiker nur verständlich, dass Online-Anbieter ihren Kunden regelmäßig eine E-Mail schicken sollten, ob diese bestimmte Daten löschen möchten. Oder aber es soll ein bestimmtes Löschedatum vereinbart werden, an dem das große Vergessen beginnt. Doch die praktische Erfahrung sieht anders aus.

5 Goldene Regeln zur Löschung von Online-Daten:

1. Füllen Sie Ihre persönlichen Profile und Benutzerkonten im Internet nur mit den zwingend erforderlichen Daten.
2. Prüfen Sie die Datenschutzerklärung der Diensteanbieter und insbesondere die Möglichkeit, das Konto später wieder löschen zu können.
3. Nutzen Sie Pseudonyme, wenn möglich.
4. Prüfen Sie alle Inhalte vor einer Veröffentlichung genau.
5. Denken Sie immer an das bleibende Gedächtnis des Internets.

Von wegen Radiergummi

Der von Politikern geforderte digitale Radiergummi für Daten im Internet will nicht so recht funktionieren. Zuerst einmal gibt es nicht den großen Knopf, mit dem sich alle persönlichen Spuren im Internet tilgen lassen. Stattdessen müssten Sie mit den jeweiligen Betreibern der Online-Angebote Kontakt aufnehmen, die Daten von Ihnen löschen sollen. Aber selbst wenn die Betreiber Ihre Daten auf den jeweiligen Internetseiten gelöscht haben, tauchen Ihre Daten an anderer Stelle wieder auf. Von einem Radiergummi kann keine Rede sein, eher von einem Stehaufmännchen.

Einmal drin, immer drin

Nicht umsonst sagen Datenschützer "Das Internet vergisst nicht." So gibt es spezielle Dienste wie das Internetarchiv www.archive.org. Sie halten sogar komplette Webauftritte vor, die es schon lange nicht mehr gibt. Damit nicht genug, haben auch die Internetsuchmaschinen ihr eigenes Gedächtnis, Cache genannt. Selbst wenn Daten von der aktuellen Webseite entfernt wurden, können sie noch im Cache einer Suchmaschine zu

finden sein. Daten im Internet können so ihre Löschung für Wochen, Monate oder gar Jahre überleben.

Verschlüsseln statt löschen?

Da es von den Daten, die im Internet veröffentlicht wurden, mitunter zahllose Kopien auf den verschiedensten Servern im Internet geben kann, ist die Löschung von Daten an nur einer Stelle leider hoffnungslos. Deshalb werden inzwischen Projekte verfolgt, bei denen personenbezogene Daten im Internet verschlüsselt werden sollen und nicht gelöscht.

Schlüssel wegwerfen reicht leider nicht

Die Idee hinter der Verschlüsselung als Ersatz für das Löschen besteht darin, dass verschlüsselte Daten nach Zerstören oder Verlust des Schlüssels nicht mehr ohne Weiteres geöffnet werden können. Wenn man also zum gewünschten Verfallsdatum den Schlüssel für seine veröffentlichten Daten löscht, könnte niemand mehr auf diese Daten zugreifen. Allerdings muss der Schlüssel vor dem Verfallsdatum der Daten verfügbar sein, damit die Daten überhaupt jemals gelesen werden können. Damit liegt ein Problem auf der Hand: Was passiert, wenn dieser Schlüssel heimlich kopiert wird? Dann könnten Unbefugte die Daten auch nach dem Verfallsdatum lesen.

Ohne Datensparsamkeit geht es nicht

Selbst wenn sich weitere Ansätze für eine Art digitalen Radiergummi finden sollten, das Internet ist zu dynamisch und zu verzweigt, um den Fortbestand von Kopien der Daten wirklich verhindern zu können. Statt einen Radiergummi zur Datenlöschung zu fordern, sollte lieber zur Datensparsamkeit aufgerufen werden. Merken Sie sich deshalb die fünf Goldenen Regeln, damit Ihre Daten so gut wie möglich im Internet vergessen werden!

Impressum

Redaktion:
Hans Mustermann
Datenschutzbeauftragter

Anschrift:
Muster GmbH
Musterstraße 12
12345 Musterstadt
Telefon:
E-Mail:

Schweigepflicht beim Betriebsarzt - kann ich wirklich sicher sein?

Sie nutzen die Möglichkeit, sich vom Betriebsarzt untersuchen zu lassen. Er weist Sie darauf hin, dass Sie Bluthochdruck haben oder auch andere Erkrankungen, die Sie lieber für sich behalten wollen. Können Sie sicher sein, dass weder Vorgesetzte noch Kollegen etwas davon erfahren?

Einen Betriebsarzt gibt es in vielen Unternehmen, teils weil dies im Arbeitssicherheitsgesetz so vorgeschrieben ist, teils als freiwilligen Service des Unternehmens.

Es gibt interne und externe Betriebsärzte

Nur große Unternehmen haben einen internen Betriebsarzt, der einen Arbeitsvertrag mit dem Unternehmen hat. Häufiger anzutreffen sind externe Betriebsärzte, die zum Beispiel eine eigene Praxis haben und daneben einige Stunden pro Woche als Betriebsarzt tätig werden. In beiden Fällen wird der Betriebsarzt vom Unternehmen bezahlt. Den einzelnen Mitarbeiter kostet der Besuch beim Betriebsarzt nichts.

Für beide gilt die ärztliche Schweigepflicht

Ein Betriebsarzt legt ärztliche Unterlagen an, genau wie das Ärzte in freier Praxis oder in einem Krankenhaus tun. Er unterliegt auch genauso wie seine Kollegen der ärztlichen Schweigepflicht. Verletzt er diese Pflicht, droht ihm ein Strafverfahren (siehe § 203 Abs. 1 Strafgesetzbuch) und außerdem ein Verfahren vor dem ärztlichen Berufsgericht.

Unterlagen des Betriebsarztes sind für den Arbeitgeber tabu

Der Betriebsarzt muss diese Unterlagen in vollem Umfang vertraulich halten. Arbeitgeber oder Vorgesetzte dürfen in keinem Fall ein Blick in die Unterlagen nehmen. Das gilt ohne Ausnahme.

Eine Besonderheit besteht allerdings: Sollte der Betriebsarzt irgendwann seine Tätigkeit für das Unternehmen beenden, dann muss er die Unterlagen im Unternehmen zurücklassen. In seiner Funktion als Betriebsarzt ist er rechtlich gesehen nämlich Teil des Unternehmens - auch als externer Betriebsarzt!

Darf der Arbeitgeber in einer solchen Situation Einblick in die Unterlagen nehmen? Natürlich nicht! Es ist lediglich erlaubt, dass der Nach-

folger des bisherigen Betriebsarztes die Unterlagen an sich nimmt. Bis das geschehen kann, müssen sie verschlossen aufbewahrt werden und dürfen von niemandem geöffnet werden.

Funktionelle Beschreibungen und Diagnosen sind zu unterscheiden

Wie sieht es mit der Information über Untersuchungsergebnisse aus? Diagnosen (also etwa "Herr A hat einen Bandscheibenvorfall") sind für den Arbeitgeber in jedem Fall tabu. Ihn haben lediglich etwaige Funktionseinschränkungen zu interessieren, die sich aus der Krankheit ergeben. Beispiel: "Herr A darf keine Lasten über 10 kg tragen."

Entscheidend ist immer der Wille des Mitarbeiters

Und was ist, wenn ein Mitarbeiter auch nicht will, dass eine solche Mitteilung erfolgt? Maßgeblich ist stets der Wille des Mitarbeiters. Wenn er dem Betriebsarzt untersagt, irgend-etwas an den Arbeitgeber weiterzugeben, dann muss sich der Betriebsarzt daran halten.

Doch Vorsicht! Zum einen kann sich ein Arbeitnehmer damit selbst schwer schaden.

Und zum anderen gibt es Fälle, in denen der Arbeitgeber einen Arbeitnehmer nur beschäftigen darf, wenn ein positives Untersuchungsergebnis vorliegt.

Beispiel LKW-Fahrer

Bekanntestes Beispiel dürften Lkw-Fahrer über 50 Jahre sein. Nur wenn die gesetzlich vorgeschriebene Tauglichkeitsuntersuchung ein positives Ergebnis hat und dieses Ergebnis dem Arbeitgeber vorliegt, darf der Beschäftigte als Lkw-Fahrer tätig sein.

Auch die Arzthelferin muss schweigen

Wie sieht es mit der Schweigepflicht aus, wenn der Betriebsarzt von einer Arzthelferin unterstützt wird? § 203 Strafgesetzbuch legt ausdrücklich fest, dass die Schweigepflicht eines Arztes auch für alle Hilfspersonen gilt, die ihn unterstützen. Sie können also sicher sein, dass auch eine Arzthelferin in keinem Fall "plaudern" wird. Sie würde sonst ein Strafverfahren riskieren und auch den Verlust ihres Arbeitsplatzes.

Lücke in der Schweigepflicht: Wer zum Betriebsarzt geht, wird manchmal gesehen

Eine Besonderheit gibt es bei der Schweigepflicht des Betriebsarztes allerdings doch: Wenn der Betriebsarzt in einem Raum des Unternehmens tätig ist, lässt es sich in aller Regel nicht verbergen, wer den Betriebsarzt aufsucht. Damit ist die Schweigepflicht nicht völlig lückenlos gewahrt. Allerdings lassen sich allein daraus im Normalfall keinerlei Schlüsse darauf ziehen, was beim Betriebsarzt gesprochen worden ist und welche Untersuchungen stattgefunden haben.

Datenschutz verletzt - und wer zahlt das Bußgeld?

Sie verstoßen gegen den Datenschutz, und plötzlich läuft gegen den Geschäftsführer Ihres Unternehmens ein Bußgeldverfahren, das bis zu 300.000 Euro kosten kann? In dieser Form sicher ein Extremfall, aber das Risiko besteht!

Zunächst ein Fall aus der Praxis: Ein Bankmitarbeiter holte bei einer Auskunft (wie etwa der SCHUFA) Bonitätsauskünfte über zwei Rechtsanwälte ein, informierte sich also darüber, wie es um ihre Zahlungsfähigkeit steht. Allerdings waren die Anwälte überhaupt keine Kunden der Bank. Das Interesse des Mitarbeiters war rein privater Natur. Die Folge: Die Datenschutzaufsichtsbehörde verhängte

ein Bußgeld von 7.500 Euro. So geschehen in Hamburg vor zwei Jahren.

Bußgeldverfahren richten sich zunächst gegen die Unternehmensleitung

Wer muss das Bußgeld eigentlich bezahlen? Die Unternehmensleitung oder der Mitarbeiter, der für den Verstoß verantwortlich ist?

Bußgeldverfahren im Datenschutzrecht haben ihre besonderen Tücken. Verstößt ein Mitarbeiter gegen Datenschutzregeln und kommt es zu einem Bußgeldverfahren, dann richtet sich das Verfahren zunächst gegen die Spitze der verantwortlichen Stelle, also gegen den Geschäftsführer oder Vorstand. Das ist logisch, denn er ist für die Aufsichtsbehörde der erste Ansprechpartner.

Im weiteren Verlauf geraten auch Mitarbeiter in den Fokus

Erst wenn genauere Ermittlungen ergeben, dass nicht ihm, sondern einem Mitarbeiter ein Fehlverhalten vorzuwerfen ist, geht die Aufsichtsbehörde auch gegen den Mitarbeiter vor und stellt das Verfahren gegen die Unternehmensleitung ein.

Sobald die Aufsichtsbehörde mit einem Bußgeldverfahren winkt, werden Geschäftsführer oder Vorstand daher genau nachbohren, wer für einen Verstoß verantwortlich ist. Denn schließlich möchten sie nicht für etwas geradestehen müssen, das sie gar nicht ausgelöst haben. Sollte der "Sünder" ermittelt werden, richtet sich das weitere Verfahren gegen ihn.

Meist kosten Verstöße um die 1.000 Euro

Was kostet denn ein typischer Datenschutzverstoß? Die meisten Bußgelder bewegen sich im Bereich von 1.000 Euro bis 2.000 Euro; das maximal mögliche Bußgeld von 300.000 Euro wurde bisher in Deutschland keine fünf Mal verhängt, und dann nie gegen einzelne Mitarbeiter, sondern gegen die Spitzen von Unternehmen. Auch muss niemand befürchten, dass wegen jeder Kleinigkeit ein Bußgeldverfahren eingeleitet wird. In ganz Deutschland kommen pro Jahr keine 50 solcher Verfahren vor, und nahezu immer geht es um wirklich gravierende Verstöße.

Probleme nicht verdrängen, sondern besprechen!

Jede Mitarbeiterin und jeder Mitarbeiter ist deshalb gut beraten, den Datenschutz nicht auf die leichte Schulter zu nehmen. Der richtige Ansprechpartner, um Zweifelsfragen zu klären, ist Ihr Datenschutzbeauftragter! Wenn also Probleme auftauchen, schweigen Sie sie bitte nicht tot! Reden Sie darüber mit Kolleginnen, Kollegen und Vorgesetzten und vereinbaren Sie, wer den Fall dem Datenschutzbeauftragten schildert. So vermeiden Sie persönliche Risiken und wehren Schaden vom Unternehmen ab.

Facebook Messages: Testen Sie, ob Sie sich der Risiken bewusst sind!

Frage: Ist es von Vorteil, nur ein Passwort für möglichst viele Dienste zu haben?

- a) Natürlich, denn dadurch fällt es mir leichter, das Passwort nicht zu vergessen.
- b) Nein, man sollte möglichst viele Passwörter verwenden, um Datendiebe zu verwirren.
- c) Es kommt auf die Stärke des Passworts an. Ist es zu schwach, sind bei nur einem Passwort gleich mehrere Dienste in Gefahr.

Lösung: Richtig ist Antwort c). Schwache Universalpasswörter sind so gefährlich wie der Zentralschlüssel einer Schließanlage, der von Unbefugten gestohlen werden kann.

Frage: Werden die Sicherheits- und Datenschutz-Optionen, die Sie in Ihrem E-Mail-Client eingestellt haben, von Facebook Messages übernommen, wenn Sie die E-Mails auf Facebook umleiten?

- a) Leider nicht. Ich muss meine Datenschutzeinstellungen auch bei Facebook machen, um meine E-Mails wie gewünscht zu schützen.
- b) Wenn ich meine E-Mails an Facebook weiterleite, werden dort sofort alle Einstellungen übernommen.

Lösung: Antwort a) ist richtig. Sie müssen die Sicherheits- und Datenschutzeinstellungen in Facebook (erneut) vornehmen.

Frage: Gilt die Datenschutzerklärung Ihres Mail-Anbieters auch für Facebook Messages, wenn Sie Ihre E-Mail darüber abrufen?

- a) Aber natürlich, danach muss sich auch Facebook richten.
- b) Für Facebook Messages gilt erst einmal nur die Datenschutzerklärung von Facebook.

Lösung: Wer b) sagt, liegt richtig. Sie müssen für jeden Dienstleister und jeden Dienst die Datenschutzerklärung separat prüfen. Facebook ist nicht an die Aussagen eines anderen Anbieters gebunden.

Frage: Drohen auch bei Facebook Messages Schadprogramme und Spam innerhalb der Nachrichten und Dateianhänge?

- a) Bei Facebook gibt es keine Viren und kein Spam.
- b) Auch Facebook kann keine Garantie geben, dass alle Nachrichten unverseucht und frei von Spam sind.

Lösung: b) stimmt auch hier, denn auch wenn Facebook versuchen wird, Spam und Schadsoftware auszufiltern, ist Facebook Messages von diesen Gefahren bedroht.

Frage: Wenn bei Facebook Messages eine Nachricht von einem Ihrer Freunde angezeigt wird, ist dann die Identität des Absenders sicher?

- a) Auch bei Facebook kann man eine falsche Identität vortäuschen.
- b) Facebook kann die Absenderangabe mit dem Online-Profil meines Freundes vergleichen. Deshalb ist die Identität sicher.

Lösung: Antwort a) ist korrekt. Weder die Nachrichten in Facebook noch die Online-Profile lassen sich mit Gewissheit einer Person zuordnen. Wer zum Beispiel in Facebook eine falsche Identität als Online-Profil einrichtet, kann diese auch als Mail-Absender verwenden.