

Newsletter Datenschutz

Die Kundenzeitung der agentia wirtschaftsdienst

Liebe Leserin, lieber Leser,

über Datenschutz wird in der letzten Zeit viel gesprochen und berichtet. An Datenschutz gedacht wird aber leider immer noch zu wenig. Diese Ausgabe Ihrer Datenschutz-Zeitung unterstreicht dies gleich mehrfach. So finden Sie auf dieser Seite einen Beitrag über meist noch unbekannt Risiken, die mit der Nutzung von Messenger-Programmen wie WhatsApp verbunden sind.

Folgen für den Datenschutz, die Fehler in der Datenverarbeitung verursachen können, müssen ebenfalls stärker ins Bewusstsein gelangen. Zudem wird häufig übersehen, was zum Beispiel auf Bildern von einem Mieterfest zu sehen sein darf und was nicht. Selbst bei klassischen Themen wie der Videoüberwachung im Bürogebäude gibt es immer noch Unklarheit darüber, was erlaubt ist und was nicht.

Über Datenschutz zu reden, reicht eben nicht - richtige Aufklärung tut Not.

Ihre *Datenschutzbeauftragten der agentia wirtschaftsdienst*

WhatsApp & Co.: kurze Nachricht, dauerhaftes Risiko

Nutzen Sie auch ein Chat-Programm wie WhatsApp? Dann wird es höchste Zeit, sich mit den Datenschutz-Optionen zu befassen. Die Berichte über unsichere Einstellungen häufen sich.

Immer im Austausch bleiben

Ob in der Straßenbahn, im Bistro oder sogar zu Fuß unterwegs, viele Smartphone-Nutzer blicken gebannt auf ihr Display. Auch wenn sie dabei so aussehen, als ob sie sich nur noch mit ihrem mobilen Endgerät befassen würden: In den meisten Fällen kommunizieren sie mit anderen Personen. Neben den sozialen Netzwerken wie Facebook sind es Messaging-Programme wie WhatsApp, die die Blicke auf sich ziehen.

Selbst der Projektstatus wird per Chat kommuniziert

Die Chat- oder Messaging-Apps werden nicht nur zum Austausch im Freundes- und Familienkreis genutzt. So manches Projektteam hat schon den Austausch über den aktuellen Status von der E-Mail-Kommunikation hin zur Kommunikation mittels WhatsApp & Co. verlagert. Als Vorteil wird unter anderem der Austausch in Echtzeit gesehen, zeitliche Verzögerungen waren gestern, denn die Kommunikationspartner sind immer online und erreichbar über ihre Chat-Dienste.

Absicherung von E-Mail reicht nicht mehr

Was leider oft vergessen wird: Während die E-Mail-Programme über Sicherheitslösungen wie Anti-Virus und Anti-Spam zusätzlich abgesichert werden, bleiben viele Chat-Anwendungen ohne zusätzlichen Schutz. Auch die Einstellungen zum Datenschutz werden nicht überprüft. Tatsächlich gibt es aber Funktionen bei Messaging-Apps, die noch mehr verraten, als dies E-Mail-Programme überhaupt tun können.

Mangelnde Sicherheit: Datenverlust und heimliche Überwachung

Die Kommunikation in Echtzeit kann ungeahnte Konsequenzen haben: Einige Chat-Apps zeigen an, ob der Nutzer gerade online ist oder nicht, teilweise wird sogar übermittelt, wann die letzte Anmeldung war und über welche Art von Gerät kommuniziert wurde. Dadurch können andere Nutzer sehen, dass Sie zum Beispiel vor 30 Minuten mit dem Smartphone angemeldet waren, jetzt aber den Desktop-PC nutzen und damit wohl nun im Büro angekommen sind.

Ein weiteres Problem der Echtzeit-Kommunikation: Alle Inhalte, die Sie mit einem Messaging-Dienst übermitteln, werden auch unmittelbar übertragen. Sie sollten also noch genauer überlegen, was Sie schreiben und verschicken wollen und was nicht. Vor der Nutzung von WhatsApp & Co sollten Sie deshalb klären, welche Datenschutz-Optionen es gibt und wie sie aktuell eingestellt sind. Sehen Sie sich vor der Anmeldung zu einem solchen Dienst immer die Datenschutzerklärung an. Überlegen Sie, wie der meist kostenlose Dienst eigentlich dem Anbieter Geld einbringt. So könnten Ihre Daten zum Beispiel zu Werbezwecken eingesetzt werden, auch Ihre Freundesliste.

Sichere Messaging-Programme

- 1) Ist das Messenger-Programm zur betrieblichen Nutzung freigegeben?
- 2) Haben Sie die Datenschutzerklärung geprüft?
- 3) Haben Sie die Datenschutz- und Sicherheitseinstellungen geprüft?
- 4) Werden die gespeicherten Daten und die Online-Verbindung verschlüsselt?

Was hat Datenqualität mit Datenschutz zu tun?

Mehr Sorgfalt bei der Datenerfassung und Datenspeicherung hilft auch dem Datenschutz. Der Aufwand für eine hohe Qualität in der Datenverarbeitung lohnt sich also gleich mehrfach.

Qualitätsmanagement und Datenschutz

Niemand freut sich wirklich, wenn man auf Fehler und mangelnde Qualität angesprochen wird. Einmal kommt die oder der Vorgesetzte, dann jemand aus der Testabteilung oder der Qualitätsmanagementbeauftragte, auch QMB genannt. Heute lesen Sie nun etwas in Ihrer Datenschutz-Zeitung zum Thema Qualität und mögliche Fehler. Das hat einen guten Grund, denn Qualitätsmanagement und Datenschutz haben viele Berührungspunkte.

Falsche Daten betreffen auch den Datenschutz

Datenschutz hat nicht nur mit der Vertraulichkeit der Daten zu tun, also damit, dass Unbefugte keinen Zugriff auf die Daten haben

dürfen. Auch die Verfügbarkeit der Daten und die Integrität der Daten spielen eine zentrale Rolle. Die Daten müssen somit auch vorhanden und auffindbar sein, und sie müssen korrekt sein. Das Bundesdatenschutzgesetz (BDSG) besagt unter anderem, dass personenbezogene Daten zu berichtigen sind, wenn sie unrichtig sind. Keine Frage, das sieht das Qualitätsmanagement genauso. Aber es geht bei der Qualität der Daten noch um mehr im Datenschutz als um die Löschung oder Sperrung falscher Daten.

Daten brauchen einen eindeutigen Speicherort

Der Datenschutz und das Qualitätsmanagement haben auch dann ein Problem, wenn die Daten planlos verstreut gespeichert werden, um einmal den Extremfall zu benennen. Einerseits kann dann nicht ausgeschlossen werden, dass es Kopien der Daten gibt, die nicht ausreichend geschützt werden. Zum anderen hängt der Schutzbedarf der Daten immer auch von ihrem aktuellen Speicherort ab. Denken Sie nur an die Diskussion rund um Cloud Computing, in der immer darauf hingewiesen wird, dass die Speicherung in der Cloud mit anderen Risiken verbunden ist als im internen Netzwerk. Zudem fordern die Datenschützer stets Klarheit darüber, wo die Daten genau gespeichert werden. Die Angabe "in der Cloud" reicht dabei nicht.

Datensicherheit braucht klare Informationen zu den Daten

Wenn Daten verschlüsselt werden sollen, um die Vertraulichkeit zu schützen, müssen alle betroffenen Datenbestände verschlüsselt werden, auch die möglichen Kopien und Backups. Das ist aber nur möglich, wenn die Verschlüsselungslösung richtig eingestellt wird, wenn alle Datenspeicherorte bekannt und für die Verschlüsselung vorgesehen sind.

Auch die Zuordnung der Daten zu bestimmten Kategorien muss stimmen: Wenn zum Beispiel eine Kundenliste nicht als solche abgelegt wird, kann es leicht passieren, dass sie bei den Schutzmaßnahmen wie der Verschlüsselung

übersehen wird. Nur mit der richtigen Ordnung können auch die Datensicherheit und der Datenschutz gelingen.

Fehler vermeiden, um Daten besser zu schützen

Doppelt erfasste Datensätze, fehlerhafte Daten, eine unordentliche Zuordnung und Speicherung von Daten haben viele negative Auswirkungen: Es entstehen unnötige Kosten bei der Datenspeicherung, Berichte und Entscheidungsvorlagen können Fehler enthalten, Kunden erhalten womöglich falsche Informationen, oder Lieferungen können an die falsche Adresse gehen, um nur einige Beispiele zu nennen.

Mangelnde Qualität bei den Daten bedroht aber auch den Datenschutz und die Datensicherheit, indem falsche personenbezogene Daten verarbeitet werden, die Daten nicht ihrem echten Schutzbedarf entsprechend abgesichert werden und Datenkopien womöglich ganz ohne Schutz verbleiben. Zur Datenqualität und zum Datenschutz gehört es auch, die Herkunft der Daten zu kennen. Denn sie sagt einerseits vielfach etwas über die Güte der Daten aus, andererseits lässt sich darüber auch die Zulässigkeit der Datenverarbeitung hinterfragen.

Achten Sie persönlich auf Datenqualität und Datenschutz

Eine höhere Datenqualität und ein besserer Datenschutz sparen unnötige Kosten und vermeiden viel Ärger zum Beispiel durch enttäuschte Kunden, die eine falsche Lieferung oder eine unberechtigte Abrechnung erhalten. Denken Sie deshalb immer an saubere und sichere Daten, beides gehört zum Datenschutz dazu.

Tipps für mehr Datenqualität und Datenschutz

Fragen Sie sich bei neuen Verfahren und Abläufen:

Woher stammen die Daten, welche Datenquellen gibt es?

Wer erfasst oder übernimmt Daten?

Welche Qualitätsrichtlinien gibt es für die Datenerfassung oder -übernahme?

Wo werden die Daten gespeichert?

Welche Richtlinien gibt es zur Datenhaltung und zur Anlage von Kopien?

Werden bei der Eingabe auch Punkte zur Qualität und Integrität der Daten berücksichtigt?

Wird bei der Weitergabe auch an mögliche Kopien gedacht, die entstehen könnten und die beim Datenmanagement berücksichtigt werden müssen?

Wird bei der Datensicherheit und bei der Datenlöschung an mögliche Kopien gedacht?

Impressum

agentia wirtschaftsdienst
dipl.-inform. udo wenzel
budapester straße 31
10787 berlin

tel.: 030 2196 4390
fax: 030 2196 4393

udo.wenzel@agentia.de
thorsten.ritter@agentia.de

Streit um Fotos vom Mieterfest

Eine Wohnbaugenossenschaft lädt einmal im Jahr alle Mieter zu einem Fest ein. Dabei lässt sie Fotos machen. Diese Fotos kommen in eine Broschüre, die zum Jahresende an alle Mieter verteilt wird. Ist das so in Ordnung, oder müsste vorher noch eine ausdrückliche Einwilligung der Personen auf den Bildern eingeholt werden? Der Bundesgerichtshof hat dazu eine klare Meinung. Sie ist auch für Fotos von Betriebsfesten wichtig.

Ein Fest für über 2.000 Mieter

Wie jedes Jahr im August lud eine Wohnbaugenossenschaft ihre weit über 2.000 Mieter zu einem Fest ein. Von einer Mieterfamilie waren Mutter, Tochter und Enkelin erschienen - ein schönes Fotomotiv mit drei Generationen auf einmal! Natürlich kam dieses Bild in die Broschüre "Informationen der Genossenschaft". Diese Broschüre erscheint einmal jährlich in einer Auflage von etwa 2.800 Exemplaren. Sie wird ausschließlich an die Mieter der Genossenschaft verteilt.

Mutter, Tochter und Enkelin wehren sich gegen ein Foto

Das Fest hatte ihnen wahrscheinlich gefallen. Von einer Veröffentlichung ihres Fotos in der Broschüre hielten die drei Damen allerdings überhaupt nichts. Sie verlangten von der Wohnbaugenossenschaft, dass sie die Verbreitung dieses Fotos künftig unterlassen solle. Außerdem forderten sie einen "Schadensersatz" in der beachtlichen Höhe von 3.000 Euro. Ihre Begründung: Die Veröffentlichung habe ihr Recht am eigenen Bild verletzt.

Der Bundesgerichtshof meint nicht, dass Unrecht geschehen wäre

Letzten Endes kam der Rechtsstreit bis zum Bundesgerichtshof. Der hatte für die Forderungen der drei Frauen allerdings gar kein Verständnis. Sowohl einen Anspruch auf Unterlassung als auch einen Anspruch auf Schadensersatz lehnte er rundheraus ab. Seine Begründung:

- Es ist richtig, dass die Veröffentlichung eines Bildes vom Grundsatz her nur dann erlaubt ist, wenn die abgebildeten Personen ausdrücklich zugestimmt haben. Dafür gibt es sogar eine eigene gesetzliche Regelung, die im Normalfall allerdings nur Spezialisten bekannt ist (§ 22 Kunsturheberrechtsgesetz).
- Ausnahmen von diesem Grundsatz gelten allerdings - und auch das steht in diesem Gesetz - dann, wenn ein Bild dem Bereich der

Zeitgeschichte zuzuordnen ist. Außerdem muss sichergestellt sein, dass die berechtigten Interessen der abgebildeten Personen nicht verletzt werden.

Das Mieterfest ist ein Ereignis der Zeitgeschichte

Ein Mieterfest gehört nach Auffassung des Gerichts zum Bereich der Zeitgeschichte. Es handle sich zwar nur um eine Veranstaltung von lokaler Bedeutung. Das genüge jedoch, da auch an einer solchen Veranstaltung ein allgemeines gesellschaftliches Interesse bestehe.

Interessen der drei Frauen verletzt das Foto nicht

Interessen der abgebildeten Personen sind nach Auffassung des Gerichts nicht verletzt:

- Das Bild dokumentiert das harmonische Zusammensein von Jung und Alt in fröhlicher und entspannter Atmosphäre.
- Es dokumentiert, dass Mitbewohner aller Altersgruppen das Fest genossen haben.
- Die Broschüre, in der das Bild enthalten ist, wird ausdrücklich nur an Mieter der

Genossenschaft verteilt. Das ist der beschränkte Personenkreis, der zu dem Fest eingeladen war.

- Die Wohnbaugenossenschaft hat ein schützenswertes Interesse daran, ihre Mieter über die Veranstaltung zu informieren.
- Die Berichterstattung, zu der das Bild gehört, vermittelt den Eindruck, dass die Mieter sich in der Genossenschaft wohlfühlen und es sich lohnt, dort Mieter zu sein.

Vorsicht: Für Fotos im Internet gelten andere Regeln!

Beachten sollte man besonders den Hinweis, dass die Broschüre mit dem Bild ausschließlich an die Mieter verteilt wird und damit ausschließlich an den Personenkreis, der selbst an dem Fest teilgenommen hat oder jedenfalls teilnehmen konnte. Hätte die Genossenschaft die Bilder beispielsweise allgemein zugänglich ins Internet gestellt, hätte der Fall durchaus anders ausgehen können.

Für Fotos von Betriebsfesten gelten ähnliche Regeln

Wie es bei Fotos von Betriebsfesten aussieht, war für den Bundesgerichtshof in diesem Fall kein Thema. Aller Voraussicht nach würde er sie jedoch ähnlich bewerten. Wenn bei einem Betriebsfest also Fotos entstehen und diese Fotos dann nur im Unternehmen selbst verbreitet werden, ist das in Ordnung. Das gilt jedenfalls für "normale" Fotos, die schlicht das fröhliche Geschehen zeigen. Anders sähe es natürlich mit Fotos von Entgleisungen aus - aber auf die Idee, sie etwa in die Betriebszeitung aufzunehmen, kommt ohnehin niemand.



*Nicht immer kann man sich gegen die Veröffentlichung von Fest-Bildern wehren
(Bild: Ingram Publishing/Thinkstock)*

Videüberwachung von Bürogebäuden - die aktuellen Spielregeln

Sie suchen Ihren Steuerberater auf. Seine Kanzlei befindet sich in einem Bürogebäude mit mehreren Stockwerken. Im Treppenhaus und in den Fluren bemerken Sie nicht weniger als zehn Videokameras. Sie fühlen sich unwohl und fragen sich: Darf das denn eigentlich sein? Lesen Sie, welche Spielregeln für solche Überwachungskameras nach neuester Rechtsprechung gelten.

Diebstähle und Schmierereien

Unter den Mietern eines Bürogebäudes gab es erhebliche Unruhe. Aus einem Büro im Erdgeschoss waren sechs Notebooks gestohlen worden. Außerdem gab es immer wieder Graffiti-Schmierereien an der Außenfassade. Schließlich hatte der Eigentümer genug. Mit Einverständnis der Mieter installierte er in den Treppenhäusern und Fluren am Anfang insgesamt zehn, später nur noch neun Videokameras.

Technische Einschränkungen und Sicherungen

Diese Kameras schalten sich automatisch ein, sobald sich etwas bewegt. Sie sind fest montiert, sodass sie immer nur denselben Bereich erfassen. Eine Zoom-Funktion ist nicht vorhanden. Nach spätestens zehn Tagen werden die Aufnahmen automatisch gelöscht. Der Zugang zu den Aufnahmen ist passwortgesichert. Das Passwort ist nur dem Datenschutzbeauftragten des Unternehmens bekannt sowie der Firma, die die Anlage installiert hat.

Abbau-Verfügung der Aufsichtsbehörde

Die zuständige Aufsichtsbehörde für den Datenschutz verfügte den Abbau der Kameras. Einzige Ausnahme: Die Kamera vor dem Büro, aus dem die Notebooks gestohlen wurden, sollte einstweilen noch installiert bleiben dürfen, aber ausgeschaltet sein müssen. Hier war sich die Behörde nämlich nicht sicher, ob die Kamera vielleicht doch notwendig war.

Das Gericht hat Verständnis für die Nöte des Eigentümers

Diese Verfügung ließ sich der Gebäudeeigentümer nicht gefallen. Er klagte dagegen, sodass die Angelegenheit schließlich beim Obergericht Lüneburg landete. Das Obergericht hatte Verständnis für seine Nöte und entschied, dass alle Ka-

meras in Betrieb bleiben dürfen. Rechtsgrundlage hierfür sei § 6b Bundesdatenschutzgesetz (Videoüberwachung öffentlich zugänglicher Räume):

- Das Bürogebäude ist öffentlich zugänglich. Beschäftigte, Kunden, Klienten, Zulieferer usw. haben nämlich freien Zugang.
- Das Bürogebäude ist "rund um die Uhr" als öffentlich zugänglich anzusehen, also auch außerhalb branchenüblicher Geschäfts- und Öffnungszeiten. Gerade in Kanzleien kommt es nämlich immer wieder vor, dass auch Termine deutlich außerhalb üblicher Zeiten vereinbart werden.
- Der Eigentümer ist Inhaber des Hausrechts am Gebäude.

- In Wahrnehmung des Hausrechts darf er die öffentlich zugänglichen Teile des Gebäudes mit Kameras überwachen. Das dient zum einen der Verhinderung von Straftaten durch Abschreckung. Zum anderen hat es den Zweck, Beweismittel für eine mögliche Strafverfolgung zu sichern.

- Wie die Vorfälle in der Vergangenheit zeigen, besteht bei dem Gebäude eine konkrete Gefährdungslage. Es geht nicht nur um eine allgemeine abstrakte Gefahrenvorsorge.

- Eine Videoüberwachung (Beobachtung und Speicherung) ist prinzipiell zur Abschreckung von Störern und Straftätern geeignet.

- Mildere, aber gleich wirksame Mittel sind nicht erkennbar. Als Alternative käme nur der Einsatz von Wachpersonal in Betracht. Wachpersonal kann jedoch nicht zu jeder Zeit an allen überwachten Stellen anwesend sein. Auch wären die Kosten hierfür wirtschaftlich nicht vertretbar.

- Die Interessen der Betroffenen sind ausreichend gewahrt. Die Kamera verfügt nicht über eine Zoom-Funktion, und auf die Bilder wird nur zugegriffen, wenn dazu Anlass besteht.

Kennen Sie die Gefahren der Echtzeit-Kommunikation?

Frage: Bei Chat-Programmen drohen keine Viren-Attacken. Stimmt das?

- a) Schadprogramme kommen nur über E-Mails, den Webbrowser oder USB-Sticks auf den Rechner.
- b) Sowohl die Chat-App als auch mögliche Dateianhänge wie zum Beispiel Bilder können mit Viren verseucht sein.

Lösung: Die Antwort b) ist richtig. Schadprogramme können über jede Form des Datenaustauschs auf Ihren PC, Ihr Notebook oder Ihr Smartphone kommen, auch bei Nutzung von Chat-Programmen.

Frage: Viele Chat-Programme können mit einem Spitznamen genutzt werden, sind also ganz anonym. Ist das richtig?

- a) Wenn ich einen Spitznamen verwende, erkennen mich nur meine Freunde.
- b) Bei der Anmeldung müssen persönliche Angaben gemacht werden. Außerdem werden die IP-Adresse meiner Internetverbindung und oftmals auch Kennungen meines Geräts übermittelt.

Lösung: Die Antwort b) ist wieder richtig. Auch wenn nur ein Spitzname in der Chat-Anwendung angezeigt wird, hat der Anbieter viele personenbezogene Angaben über den Nutzer. Es ist deshalb sehr wichtig, die Datenschutzerklärung zu prüfen. Zudem werden häufig Kontaktdaten der Freunde und Kommunikationspartner in die Anwendung übertragen. Alle gespeicherten Daten sollten deshalb verschlüsselt sein, auch gegenüber dem Betreiber des Messaging-Dienstes.