SANOVIS CONSULTING WITH CARE.

CURACON SICHERHEIT GEBEN. LÖSUNGEN BIETEN.

NEWSLETTER DATENSCHUTZ

Liebe Leserin, lieber Leser,

Fehler im Umgang mit personenbezogenen Daten können ungeahnte Folgen haben, nicht nur für die betroffenen Personen, auch für die Verursacher. Erfahren Sie deshalb in dieser Ausgabe, warum die unerlaubte Nutzung von E-Mail-Adressen zu Schadensersatzansprüchen führen kann. Auch der Missbrauch von anderen Unternehmensdaten für private Zwecke kann ernsthafte Konsequenzen nach sich ziehen.
Wie die neue Ausgabe zeigt, kann bereits die Einrichtung einer Messenger-App zu einer Datenschutzverletzung führen. Es lohnt sich also, sich genau über die Vorgaben des Datenschutzes zu informieren, auch zum Beispiel über die Bedeutung von Vertraulichkeit im Datenschutz.
Die Lektüre Ihres Datenschutz-Newsletters ist der richtige Weg, um ungewollte Datenschutz-Pannen zu vermeiden. Sie erfahren prägnant und auf den Punkt, worauf es im Datenschutz ankommt und welche Vorteile gelebter Datenschutz mit sich bringt.
Wir wünschen Ihnen interessante Erkenntnisse beim Lesen!

Dr. Uwe Günther
Beratungsfeldleiter Datenschutz, Curacon GmbH
Geschäftsführer, Sanovis GmbH

Stefan Strüwe
Beratungsfeldleiter Datenschutz, Curacon GmbH

Februar_2022

1 SCHADENSERSATZ
FÜR UNERLAUBTE E-MAILS

Jemand bekommt eine Werbemail, obwohl er Werbemails deutlich abgelehnt hatte. Jetzt möchte er wegen dieser einen Mail Schadensersatz. Hat er damit eine Chance?

Ein Versehen ist schnell passiert

Werbeverbote in eine Adressdatenbank einzutragen, ist eine lästige Arbeit. Da passiert schnell einmal ein Fehler. Und schon ist eine Werbemail verschickt, obwohl der Adressat ausdrücklich keine Werbemails haben will.

Manche wollen dafür Geld sehen

Eine freundliche Entschuldigung sollte doch wohl reichen? Manche Betroffene akzeptieren sie und alles ist gut. Es gibt aber auch betroffene Personen, die Schadensersatz verlangen. Häufig bewegen sich die Forderungen im Bereich von 100 Euro bis 300 Euro. Wohlgemerkt, wegen einer einzigen E-Mail. Bevor es die Datenschutz-Grundverordnung (DSGVO) gab, hätte jedes Gericht über eine solche Idee den Kopf geschüttelt.

Natürlich besteht ein Anspruch auf Unterlassung

Auch damals gewährten die Gerichte schon einen Anspruch auf Unterlassung. Das ist heute noch genauso. Man muss also in einer „Unterlassungserklärung“ versprechen, dass so etwas nicht wieder passieren wird. Mit dieser Erklärung muss das „Versprechen einer Vertragsstrafe“ kombiniert sein. Wird doch wieder eine E-Mail verschickt, ist das Unterlassungsversprechen gebrochen. Das wiederum löst eine Vertragsstrafe aus. Vorher ist sie kein Thema.

Schadensersatz gab es früher aber nicht

Schadensersatz wegen der einen Mail, die schon verschickt wurde, gewährten die Gerichte früher nicht. Das typische Argument lautete: Ein Schaden, den man finanziell beziffern könnte, ist nicht entstanden. Und Anlass für so etwas wie Schmerzensgeld sahen die Gerichte wegen einer solchen Kleinigkeit nicht.

Die DSGVO hat das geändert

Durch die DSGVO hat sich das geändert. Sie enthält in ihrem Artikel 82 eine Regelung über das „Recht auf Schadensersatz“. Schadensersatz gibt es demnach immer dann, wenn „wegen eines Verstoßes gegen diese Verordnung“ ein Schaden entstanden ist. Dabei kann dieser Schaden ausdrücklich materiell oder immateriell sein. Materiell bedeutet, dass er finanziell zu beziffern ist. Immateriell ist ein Schaden, wenn er sich zwar nicht in Geld messen lässt, aber doch „wehtut“.

Ein „ungutes Gefühl“ kann ein immaterieller Schaden sein

Ein typisches Beispiel für einen immateriellen Schaden sind Schmerzen. Schmerzen wird eine unzulässige Werbe-E-Mail kaum jemals auslösen. Eine gewisse Belästigung kann sie aber schon darstellen. Auch kann sie eine Unsicherheit darüber auslösen, ob die Mailadresse noch irgendwohin weitergegeben worden ist.

Ein Amtsgericht gewährte dafür 300 Euro

Tatsächlich hat ein Amtsgericht folgende Auffassung vertreten: „Der Schaden kann bereits in dem unguten Gefühl liegen, dass personenbezogene Daten Unbefugten bekannt geworden sind.“ Das war dem Gericht Anlass genug, 300 Euro Schadensersatz zu gewähren.

Beachten Sie alle Vorgaben Ihres Arbeitgebers genau

Jede und jeder sollte deshalb unbedingt die Vorgaben beachten, die im Unternehmen für den Umgang mit Mailadressen bestehen. Sonst kann es schnell teuer werden.

2 MISSBRAUCH VON DATEN

FÜR PRIVATE ZWECKE

Wer in einem Unternehmen arbeitet, hat normalerweise Zugang zu Daten von Kunden. Jedem ist klar, dass er diese Daten nicht für private Zwecke nutzen darf. Aber was sind die Folgen, wenn das trotzdem einmal geschieht? Mit einer Geldbuße dürften die wenigsten rechnen.

Nehmen wir einfach einmal an …

Angenommen, Sie haben von jemandem noch Geld zu bekommen. Leider ist Ihr Schuldner inzwischen umgezogen. Sie wissen nur nicht, wohin. Sie vermuten, dass er zu den Kunden Ihres Arbeitgebers gehören könnte. Und tatsächlich: Ein Blick in die Kundendatenbank bestätigt das. Mit einem Mausklick haben Sie seine neue Adresse gefunden.

Auch wenn Sie das sicher nie tun würden: Nehmen wir einmal an, Sie benutzen seine neue Adresse, um mit ihm wegen der Geldsache Verbindung aufzunehmen. Welche rechtlichen Folgen kann das haben?

Der Grundsatz der Zweckbindung ist verletzt

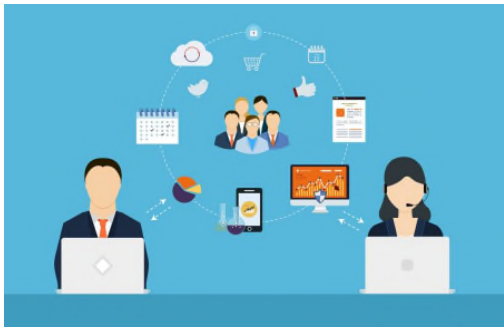
Es liegt auf der Hand, dass hier der Grundsatz der Zweckbindung verletzt ist. Der Kunde hat seine Daten dem Unternehmen genannt, damit das Unternehmen die Daten verwendet. Es braucht sie beispielsweise, um Bestellungen zu bearbeiten und auszuliefern. Nie würde der Kunde auf die Idee kommen, dass ein Mitarbeiter oder eine Mitarbeiterin diese Daten für irgendwelche privaten Zwecke „abzweigt“. Dafür waren sie nicht gedacht. Deshalb kann es gut sein, dass sich der Kunde bei der Datenschutzaufsicht beschwert.

Die Datenschutzaufsicht kann Geldbußen verhängen

Die Datenschutzaufsicht wird sich um den Fall kümmern. Seit die DSGVO gilt, hat die Datenschutzaufsicht viel mehr Befugnisse als vorher. Unter anderem kann sie Geldbußen verhängen. Das kann im Einzelfall richtig teuer werden. Einige Hundert Euro sind sehr schnell fällig. Das gilt natürlich auch, wenn jemand Daten des Arbeitgebers für private Zwecke missbraucht.

Wer muss mit einer Geldbuße rechnen?

Interessant ist dabei die Frage, wer für diesen Datenmissbrauch geradestehen muss. Ist es die beschäftigte Person, die die Daten missbraucht hat? Oder ist es der Arbeitgeber, für den sie tätig ist? Die Meinungen hierzu gehen zwischen den Aufsichtsbehörden auseinander.



Ein „Mitarbeiterexzess“ ist eine hässliche Sache

Die meisten Aufsichtsbehörden sprechen in einem solchen Fall von einem „Mitarbeiterexzess“. Gemeint sind damit nach einer gängigen Definition „Handlungen von Beschäftigten, die bei verständiger Würdigung nicht dem Kreis der jeweiligen unternehmerischen Tätigkeit zugerechnet werden können.“ Das hört sich zwar etwas juristisch an. Aber eigentlich ist ziemlich klar, was damit gemeint ist.

Ständige Überwachung soll nicht sein

Kein Arbeitgeber kann ständig hinter jedem Beschäftigten stehen. Und er soll das auch gar nicht tun. Deshalb kann der Arbeitgeber nicht für alles verantwortlich sein, was ein Beschäftigter an seinem Arbeitsplatz treibt. Wenn der Beschäftigte sich dort um rein private Angelegenheiten kümmert, ist das keine Sache des Arbeitgebers. Dafür muss vielmehr der Beschäftigte selbst geradestehen. Das gilt auch dann, wenn der Beschäftigte seine Möglichkeiten missbraucht, auf dienstliche Daten zuzugreifen.

Die Geldbuße dafür muss der Beschäftigte zahlen

Beim Missbrauch von Daten für private Zwecke hat das für den „Täter“ erhebliche Konsequenzen. Er wird durch diesen Missbrauch selbst zu der Stelle, die für den Umgang mit den Daten verantwortlich ist. Damit haftet er selbst für den Missbrauch der Daten. Die Datenschutzaufsicht kann gegen ihn persönlich ein Bußgeldverfahren einleiten und eine Geldbuße verhängen. 200 oder 300 Euro Geldbuße sind in solchen Fällen die untere Grenze. Es kann auch teurer werden.

Eine Geldbuße für den Arbeitgeber ist keine schöne Alternative

Letztlich noch unangenehmer wird es für den Beschäftigten, wenn eine Aufsichtsbehörde den Vorgang nicht als „Mitarbeiterexzess“ behandelt. Auch dann hat er selbstverständlich rechtliche Folgen. Sie richten sich gegen das Unternehmen. Denn irgendjemand muss natürlich für den Verstoß geradestehen. Und wenn es nicht der Mitarbeiter ist, ist es eben das Unternehmen.

In solchen Fällen gilt der Grundsatz: Unternehmen haften für das Fehlverhalten ihrer Beschäftigten. Deshalb wird die zuständige Datenschutzaufsicht eine Geldbuße gegen das Unternehmen verhängen.

Der Arbeitgeber wird Konsequenzen ziehen

Selbstverständlich wird das Unternehmen dies nicht einfach schulterzuckend zur Kenntnis nehmen. Vielmehr wird es das Fehlverhalten intern aufklären, arbeitsrechtliche Konsequenzen eingeschlossen. Deshalb gilt: Finger weg von dienstlichen Daten für private Zwecke! Das gilt auch dann, wenn es um scheinbar banale Daten wie eine Adresse geht. Die Folgen sind es auch hier nicht wert.

3 MESSENGER-APPS:

SCHNELLE NACHRICHT, HOHES RISIKO?

Messenger-Anwendungen wie WhatsApp und Facebook Messenger sind beliebt. Denn sie ermöglichen eine schnelle, unkomplizierte Kommunikation. Leider können solche Chat-Programme aber auch zum Datenrisiko werden, sowohl bei privater Kommunikation als auch bei beruflichen Chats.

Bekannt, beliebt, bedrohlich?

Es vibriert, es plingt, es piept: Wer in Deutschland ein Smartphone oder Handy nutzt, bekommt durchschnittlich 13 Kurznachrichten pro Tag, so eine Umfrage des Digitalverbands Bitkom.

„Kurznachrichten spielen nicht nur in der privaten Kommunikation eine ganz zentrale Rolle. Insbesondere während der Corona-Pandemie halten viele so den Kontakt zu Freunden und Familienmitgliedern und können so schnell und unkompliziert Grüße, Fotos und auch Videos austauschen“, sagt Bitkom-Hauptgeschäftsführer Dr. Bernhard Rohleder.

Wer ein Smartphone hat, greift fast immer auch auf Messenger-Dienste wie WhatsApp, Signal oder Threema zurück. 9 von 10 (88 Prozent) Nutzerinnen und Nutzern von Smartphones verwenden entsprechende Apps. Das entspricht rund 50 Millionen Menschen in Deutschland.

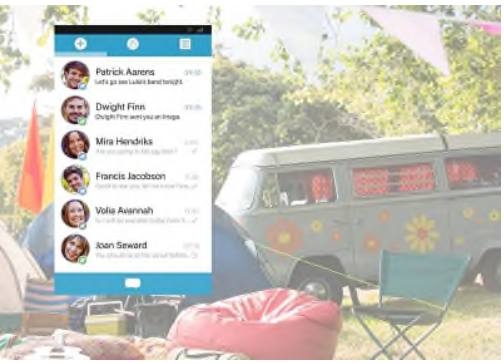
Berufliche Kommunikation findet ebenso über Messenger-Apps wie WhatsApp, Signal oder Telegram statt wie das Verschicken von Urlaubsgrüßen. 36 Prozent machen zum Beispiel im Urlaub einen Bewegtbild-Anruf per Skype, Facetime oder WhatsApp.

Messenger sind inzwischen das am häufigsten genutzte Kommunikationsmittel. Umso wichtiger ist, dass Kommunikation über Messenger in einem absolut vertrauensvollen und sicheren Umfeld stattfinden kann, wie der Digitalverband Bitkom betont.

Datenschützer weisen auf zahlreiche Risiken bei Messengern hin

Gerade der besonders beliebte Dienst WhatsApp ist häufig in der Datenschutz-Kritik. Ein Problem: Bereits bei der Anmeldung zu WhatsApp können alle Kontaktdaten, die jemand im Telefon gespeichert hat, an den Anbieter übertragen werden. Hierfür besteht weder eine Rechtsgrundlage noch können die Personen, die im Nutzertelefon gespeichert sind, in die Datenweitergabe einwilligen oder ihr widersprechen, warnen die Aufsichtsbehörden für den Datenschutz.

„Es gibt deutlich datensparsamere Messenger-Dienste auf dem Markt, die dieselben Möglichkeiten der Kommunikation bieten“, so zum Beispiel die Landesbeauftragte für den Datenschutz (LfD) Niedersachsen, Barbara Thiel.



Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen hat bereits sogenannte „Leitplanken für die Auswahl von Messenger-Diensten“ veröffentlicht, um bei der Auswahl geeigneter Messenger-Apps zu helfen (als PDF abrufbar unter https://ogy.de/leitplanken-ldi-nrw).

Worauf es bei Messengern ankommt

Vor der Entscheidung für einen Messenger-Dienst sollten Sie deshalb prüfen,

- ob der Anbieter Sie transparent über die Datenverarbeitung, die mit der Nutzung verbunden ist, informiert (Datenschutzerklärung),
- ob der Anbieter die Datenschutz-Vorgaben zur (Nicht-)Weitergabe und (Nicht-)Auswertung personenbezogener Daten einhält,
- ob die personenbezogenen Daten in ein Land außerhalb der EU übertragen werden sollen,
- ob datenschutzfreundliche Einstellungen möglich sind oder besser noch voreingestellt sind,
- ob Sie die Messenger-App nutzen können, ohne die im Adressbuch vorhandenen Kontaktdaten, insbesondere Telefonnummern, für Zwecke des Anbieters bzw. für fremde Zwecke an den Anbieter zu übermitteln, und
- ob der Anbieter übermittelte Daten mit allgemein anerkannten und dem Stand der Technik entsprechenden Verfahren verschlüsselt.

Nur freigegebene Messenger nutzen und Privatsphäre schützen

Offensichtlich bestehen zahlreiche Anforderungen an Messenger-Dienste, da es vielfältige Datenrisiken bei der Installation und Nutzung geben kann.

Verwenden Sie deshalb beruflich nur dann Messenger-Apps, wenn sie intern freigegeben sind, und dann auch nur die wirklich zugelassenen. Privat sollten Sie sich ebenfalls genau überlegen, wem Sie Ihre Kontaktdaten, Fotos, Videos und Statusinformationen anvertrauen. Es ist nicht einfach, selbst die Einhaltung der Datenschutzvorgaben zu überprüfen. Deshalb sind die Hinweise der Aufsichtsbehörden für den Datenschutz zu einzelnen Messenger-Diensten wertvoll und hilfreich, wie zum Beispiel in den erwähnten „Leitplanken für die Auswahl von Messenger-Diensten“.

Selbst wenn besonders beliebte und bekannte Messenger weit verbreitet sind, bedeutet das nicht, dass diese Messenger-Apps besonders sicher und datenschutzfreundlich sind. Sprechen Sie auch im privaten Umfeld über den Datenschutz bei Messengern und entscheiden Sie sich gemeinsam mit Ihren Kontakten für mehr Datenschutz bei der digitalen Kommunikation!

4 WAS GENAU VERSTEHT MAN IM DATENSCHUTZ UNTER VERTRAULICHKEIT?

Sicher ist Ihnen der Begriff „Vertraulichkeit“ mehr als bekannt, vielleicht sogar aus dem Bereich IT und IT-Sicherheit. Doch bedeutet Vertraulichkeit im Datenschutz auch das, was Sie sich darunter vorstellen? Gerade Alltagsbegriffe können schnell zu Unschärfen oder Missverständnissen führen.

Einmal ganz im Vertrauen gesagt

Vielleicht wundern Sie sich über die Frage, was man denn genau unter Vertraulichkeit im Datenschutz versteht. Offensichtlich geht es im Datenschutz in vielen Fällen darum, Vertrauliches zu schützen, nämlich die personenbezogenen Daten, die nicht jeder sehen, lesen und kennen darf.

Ein gutes Beispiel sind Gesundheitsdaten, die kein Dritter kennen soll. Sie gehen nur Sie, Ihre Ärztin oder Ihren Arzt oder die Krankenversicherung etwas an, aber sicherlich nicht einen Pharma-Hersteller oder den Betreiber einer Drogeriekette.

Datenschutz und Vertraulichkeit hängen tatsächlich eng zusammen. Doch Datenschutz ist mehr als Vertraulichkeit. So müssen personenbezogene Daten nicht nur vertraulich, sondern auch verfügbar sein, sie dürfen nicht manipuliert werden, und die Dienste, mit denen die personenbezogenen Daten verarbeitet werden, müssen vor Ausfällen und Störungen geschützt sein.

Was aber bedeutet nun genau die Vertraulichkeit im Datenschutz?

Es geht um Verschwiegenheit und Zugangsschutz

Zum einen gehört es zur Vertraulichkeit im Datenschutz, dass die Beschäftigten und die beauftragten Dienstleister, die personenbezogene Daten verarbeiten, keine personenbezogenen Daten an unbefugte Dritte verraten, also verschwiegen sind. Das gilt auch für die Datenschutzbeauftragten selbst.

Dann darf niemand die zu schützenden Daten unerlaubt oder ungewollt offenlegen. Unbefugte Dritte dürfen keinen Zugang zu und Zugriff auf die Daten haben. Um das zu erreichen, fordert der Datenschutz geeignete technische und organisatorische Schutzmaßnahmen. Dazu gehört vor allem eine Verschlüsselung, die dem aktuellen Stand der Technik entspricht, also nicht veraltet ist.

Die IT hat ein etwas anderes Bild von Vertraulichkeit

Vielleicht arbeiten Sie in der IT oder IT-Sicherheit, oder Sie wissen einfach, dass auch die IT-Sicherheit das sogenannte Schutzziel Vertraulichkeit besitzt. Tatsächlich nutzt die IT-Sicherheit ähnliche oder sogar die gleichen Schutzmaßnahmen wie der Datenschutz, insbesondere die Verschlüsselung.

Ist deshalb Vertraulichkeit in Datenschutz und IT-Sicherheit wirklich das Gleiche? Nicht ganz, denn der Datenschutz will personenbezogene Daten schützen, die IT-Sicherheit generell Daten mit entsprechendem Schutzbedarf.

Dabei müssen personenbezogene Daten wie die Daten eines IT-Nutzers aus Sicht der IT nicht zwingend einen hohen Bedarf an Vertraulichkeit haben. Es kann der IT-Sicherheit um einen anderen Schutzbedarf gehen.

Dem Datenschutz aber geht es immer um die Daten, die personenbezogen sind, also zu einer Person gehören, oder die personenbeziehbar sind, sich also auf eine bestimmte Person beziehen lassen. Solche Daten dürfen nicht ungewollt oder unerlaubt offengelegt werden, wie in dem Eingangsbeispiel die Gesundheitsdaten. Sie dürfen nicht einfach einem Händler übergeben werden, der diese Daten für ein passendes

Angebot an frei verkäuflichen Medikamenten nutzen möchte.

Vertraulichkeit ist deshalb ein Kernthema für den Datenschutz, mit gewissen Unterschieden zur Sicht der IT oder auch zur Alltagssicht.

Ist Ihnen Vertraulichkeit im Datenschutz ein Begriff? Machen Sie den Test!

Vertraulichkeit, Verschwiegenheit und Datenschutz sind eigentlich identisch. Stimmt das?

1. Nein, Vertraulichkeit ist zentral für den Datenschutz. Aber es geht auch um andere Datenschutz-Prinzipien, die zu wahren sind.
2. Ja, es geht immer darum, Geheimnisse zu wahren.

Lösung:

Die Antwort 1. ist richtig. Die Datenschutz-Grundverordnung (DSGVO) nennt mehrere Grundsätze für die Verarbeitung personenbezogener Daten. Vertraulichkeit gehört dazu, ist aber nicht alles im Datenschutz. Geheimnisse wie zum Beispiel Geschäftsgeheimnisse müssen keinen Personenbezug haben und unter-liegen dann nicht dem Datenschutz. Zudem müssen personenbezogene Daten nicht geheim sein, um schutzbedürftig zu sein. Auch personenbezogene Daten, die nicht geheim sind, dürfen beispielsweise nicht zweckentfremdet werden.

Sorgt die IT für Vertraulichkeit, stimmt auch der Datenschutz. Ist das so richtig?

1. Ja, IT-Sicherheit sorgt für die Vertraulichkeit, die der Datenschutz braucht.
2. Nein, IT-Sicherheit und Datenschutz haben unterschiedliche Ziele. Die IT-Sicherheit schützt nicht automatisch personenbezogene Daten.

Lösung:

Die Antwort 2. ist richtig. IT-Sicherheit soll Systeme und Daten schützen, die für den IT-Betrieb wichtig sind oder die anderweitig geschäftsrelevant sind. Für den Datenschutz geht es darum, die Vertraulichkeit personenbezogener und personenbeziehbarer Daten sicherzustellen. Es kann deshalb sein, dass die IT-Sicherheit umfangreich Nutzerdaten analysiert, um Attacken zu erkennen, während der Datenschutz versucht, möglichst den Personenbezug bei den Analysen zu vermeiden.

IMPRESSUM

Redaktion
Dr. Uwe Günther
Sanovis GmbH
Riedenburger Straße 7
81677 München
089 9927579-22
Uwe.Guenther@Sanovis.com

Stefan Strüwe, RA
CURACON GmbH Wirtschaftsprüfungsgesellschaft
Am Mittelhafen 14
48155 Münster
0251 92208-209
Stefan.Struewe@Curacon.de