

Datenschutz bei Smartphone-Apps – Worauf Sie achten sollten –

Ihr Datenschutz-Info Blatt



Liebe Leserin, lieber Leser,

viele Verstöße gegen die Vorgaben des Datenschutzes geschehen aus Unwissenheit. Genau das soll Ihnen nicht passieren! Deshalb erfahren Sie in der neuen Ausgabe unserer Datenschutz-Zeitung, wie Sie richtig reagieren, wenn einmal Ihr Firmen-PC nicht funktioniert und Sie gern auf Ihr privates Notebook zurückgreifen würden.

Welche Folgen eine Verletzung des Datenschutzes haben kann, lesen Sie in einem weiteren Beitrag. Er klärt über mögliche Schadensersatzansprüche auf.

Man kann nie genug über seine Daten wissen, so könnte man denken. Doch alles hat seine Grenzen, auch der Auskunftsanspruch aus dem Datenschutzrecht. Allerdings haben Sie immer das Anrecht auf eine Datenschutzerklärung, wenn Sie eine App nutzen möchten. Erfahren Sie deshalb, wie es um Datenschutzhinweise bei mobilen Anwendungen steht.

Ich wünsche Ihnen viel Spaß beim Lesen!

Ihr Frank Berns, Datenschutzbeauftragter

Wenn der Firmen-Rechner streikt: Private Geräte als Notfallstrategie?

Der Rechner, den der Arbeitgeber zur Verfügung gestellt hat, fährt nicht hoch. Doch es steht eine dringende Projektarbeit an. Da kommt schnell der Gedanke, das private Notebook zu nutzen. Es handelt sich ja um einen Notfall. Doch stimmt dann auch der Datenschutz?

Immer wenn es eilig ist

Wie könnte es anders sein? Um elf Uhr soll das Konzept bei der Abteilungsleiterin sein, aber der PC, den der Arbeitgeber für die Tätigkeit im Homeoffice bereitgestellt hat, startet nicht. Nur noch zwei Stunden bis zur Abgabe.

Eigentlich ist die Nutzung privater IT-Geräte bei der Heimarbeit ja nicht erlaubt. Der Arbeitgeber hat daher extra spezielle PCs angeschafft und den Beschäftigten nach Hause liefern lassen. Aber jetzt ist eine Art Notfall eingetreten: Der Firmen-Computer will nicht, da könnte man doch das private Gerät nutzen. So zumindest die Idee, die einem in den Kopf kommt. Immerhin war das private Notebook ja teuer, es ist schon sehr professionell, muss man sagen ...

Der PC-Streik und die Folgen

Wer einfach das private Notebook verwendet, um das Konzept fertigzustellen, hält vielleicht die gesetzte Frist zur Abgabe ein – doch er verstößt gegen die Richtlinien, die der Arbeitgeber für die Arbeit im Homeoffice aufgestellt hat.

Gehen Sie nicht davon aus, dass die „Frist“ alle Mittel heiligt. Das Konzept ist zwar möglicherweise pünktlich bei der Abteilungsleiterin. Aber das vertrauliche Konzept mit den Kundendaten ist auf einem privaten Gerät gelandet. Sie haben es dort bearbeitet und von dort per Mail verschickt.

Der Arbeitgeber hat die Nutzung des privaten Geräts nicht einfach so verboten. Es gibt gute Gründe dafür. Der Arbeitgeber hat keinen Überblick darüber,

- ob das private Notebook mit allen Updates versehen ist,
- ob die Sicherheitssoftware darauf den Anforderungen entspricht,
- ob der Mail-Versand geschützt erfolgt oder
- ob das private Notebook zum Beispiel so eingestellt ist, dass alle Dateien darauf automatisch zur Datensicherung in eine Cloud übertragen werden, die nicht den Vorgaben des Datenschutzes entspricht.

Erst fragen und Schutz sicherstellen

Wer ohne Rücksprache von den Sicherheitsrichtlinien des Arbeitgebers abweicht, muss mit Ärger rechnen, auch wenn es um ein dringendes Konzept geht und wenn man für den Notfall eine Ausnahme machen wollte.

Sichern Sie sich grundsätzlich immer selbst ab und fragen Sie die Vorgesetzten, ob Sie das private Gerät für diesen Fall ausnahmsweise nutzen dürfen. Denken Sie dann aber auch an die Absicherung der Daten.

So sollte der Arbeitgeber die Nutzung privater IT, auch BYOD (Bring Your Own Device) genannt, wenn überhaupt nur dann genehmigen, wenn die Maßnahmen für Sicherheit und Datenschutz bei dem Gerät stimmen. Es muss die gleiche hohe Sicherheit herrschen, als wenn Sie den Firmen-PC nutzen würden.

Genehmigt der Arbeitgeber die Ausnahme, müssen alle Schutzmaßnahmen ergriffen werden, die den Zugang auf das Firmennetzwerk absichern und die dafür sorgen, dass keine betrieblichen Daten auf den privaten Geräten zurückbleiben.

Wenn Ausnahme, dann aber nicht die Regel

Hat der Arbeitgeber einmal zugelassen, dass Sie Ihr privates Gerät nutzen, darf sich daraus aber keine Regel entwickeln, weil Sie zum Beispiel mit dem privaten Notebook lieber arbeiten würden.

Schadensersatz bei Verletzungen des Datenschutzes



Verstöße gegen den Datenschutz führen schnell zu Schadensersatzansprüchen. Grund genug, es mit den Regeln des Datenschutzes sehr genau zu nehmen!

2.000 € Schmerzensgeld sind keine Kleinigkeit

Wer an seinem Arbeitsplatz Mails versendet, sollte die Spielregeln des Datenschutzes kennen, die dabei gelten. Und: Extrem sorgfältiges Arbeiten ist angesagt! Das hätte der Mitarbeiter einer Krankenversicherung besser beherzigen sollen. Denn wegen einer gar nicht so großen Datenschutzpanne muss sein Arbeitgeber jetzt 2.000 € Schmerzensgeld zahlen.

„Fehlversendungen“ passieren bei Mails sehr schnell

Mails sind schneller als Briefpost und auch billiger. Das gilt allerdings nur, wenn die Mail an die richtige Adresse geht. Ein „Fehlversand“ an eine falsche Adresse kann erheblichen Ärger nach sich ziehen. Genau eine solche Panne unterlief dem Mitarbeiter einer Krankenversicherung.

Ein Sachbearbeiter verschreibt sich bei der Mailadresse

Eine Kundin meldete sich bei ihm telefonisch und bat darum, ihr den Inhalt ihrer Gesundheitsakte aus den letzten drei Jahren zuzusenden. Der Mitarbeiter fragte die Kundin, ob eine Zusendung per Mail in Ordnung wäre.

Anfangs hatte die Kundin Bedenken, schließlich stimmte sie aber zu. Dabei war ihr klar, dass ihr eine unverschlüsselte Mail zugehen würde. Sie bat darum, ihr die Unterlagen an die Mailadresse „B1@fff.de“ zu senden. Aus Versehen schrieb der Sachbearbeiter jedoch an „B2@fff.de“.

Natürlich entschuldigt er sich bei der Kundin

Erst als sich die Kundin nach drei Tagen erkundigte, wo denn die Mail mit ihren Unterlagen bleibt, fiel die Panne auf. Der Sachbearbeiter entschuldigte sich bei der Kundin. Außerdem informierte er seine Vorgesetzten.

Ein wirtschaftlicher Schaden ist nicht entstanden

Letztlich „passierte nichts“. Einige Monate später kontaktierte ein Mitarbeiter der Krankenkasse das Unternehmen, das sich in den beiden Mailadressen hinter der Abkürzung „fff“ verbirgt. Das Unternehmen „fff“ versicherte, dass das E-Mail-Postfach „B2fff.de“ nie benutzt worden sei. Man habe es jetzt gelöscht.

Die Kundin fordert 15.000 € und bekommt 2.000 €

Trotzdem forderte die betroffene Kundin Schmerzensgeld. Ihre Vorstellung: 15.000 €, Anwaltskosten natürlich extra. Das Oberlandesgericht Düsseldorf stutzte zwar die Hoffnungen der Kundin erheblich zurecht. 2.000 € Schmerzensgeld bewilligte das Gericht ihr aber doch.

Es geht um Ausgleich für Sorgen und Ängste

Nach Auffassung des Gerichts soll das Schmerzensgeld die Kundin für die Sorgen und Befürchtungen entschädigen, unter denen sie gelitten hat. Denn immerhin habe sie viele Monate lang die Kontrolle über sensible Gesundheitsdaten verloren. Zudem seien diese Daten zum Teil sogar ausgesprochen intim gewesen.

Der Hinweis auf ein bloßes Versehen hilft nichts

Dass dem Sachbearbeiter erkennbar „nur“ ein Versehen passiert war, half nichts. Damit befasste sich das Gericht noch nicht einmal näher. Es stellte einfach fest, dass der Versand an die falsche Mailadresse den Datenschutz verletzt hat.

Zwar war die Kundin mit einer Versendung per Mail einverstanden, aber natürlich nur mit einer Versendung an die richtige Mailadresse. Da der Sachbearbeiter eine andere Mailadresse benutzte, bleibt es dabei, dass ein Datenschutzverstoß vorlag.

Aufmerksamkeit bei Datenschutz-Schulungen macht Sinn

Der Fall erinnert daran, dass man an Datenschutz-Schulungen sehr aufmerksam teilnehmen sollte. Gibt es vielleicht Daten, die überhaupt nicht per Mail verschickt werden sollen? Wie stelle ich sicher, dass die Mailadresse auch wirklich stimmt? Wer hier aufpasst und auch einmal nachfragt, bewahrt sein Unternehmen vor Schadensersatzansprüchen und sich selbst vor Ärger!

Briefpost kann genauso riskant sein

Da per Mail alles so gründlich schiefgegangen war, schickte die Krankenkasse der Kundin die angeforderten Unterlagen schließlich per Brief. Verständlich, denn von Mails hatten in diesem Fall beide Seiten genug. Gerade deshalb sollte man bedenken: Eine falsche Adressierung kommt sehr wohl auch bei Briefen vor, und zwar gar nicht so selten. Auch dann ist Schadensersatz fällig.

Jedenfalls eine Abmahnung steht noch im Raum

Die 2.000 € muss die Krankenkasse zahlen, nicht der Sachbearbeiter persönlich. Ob sein Arbeitgeber bei ihm Rückgriff nehmen kann, richtet sich nach den Regeln des Arbeitsrechts. Da der Sachbearbeiter „nur“ fahrlässig gehandelt hat, wird er seinem Arbeitgeber wahrscheinlich nichts erstatten müssen.

Eine Abmahnung wäre aber allemal gerechtfertigt. Sollte es früher schon weitere Verstöße gegeben haben, stünde auch eine Kündigung im Raum.

Auskunftsanspruch für Kontoauszüge?

Das Recht auf Auskunft ist vielleicht das wichtigste Recht in der Datenschutz-Grundverordnung (DSGVO). Aber auch dieses Recht hat Grenzen. Am Beispiel von Kontoauszügen lässt sich das sehr schön zeigen.

Das Auskunftsrecht ist sehr wichtig

Eine betroffene Person hat bekanntlich ein Recht auf Auskunft über alle Daten, die sie betreffen. Klar ist auch, wie wichtig dieses Recht ist. Nur wenn jemand weiß, ob etwa ein Unternehmen Daten über ihn verarbeitet, kann er nachprüfen, ob damit alles in Ordnung ist.

Es gibt auch ein Recht auf eine Kopie

Geregelt ist das alles in Art. 15 DSGVO. Dort ist auch festgelegt, dass eine betroffene Person „eine Kopie der personenbezogenen Daten“ verlangen kann. An dieser Formulierung entzündete sich ein Streit zwischen einer Bank und einem ihrer Kunden.

Die erste Kopie ist kostenlos

Der Kunde hatte seine Kontoauszüge offensichtlich völlig korrekt erhalten. Allerdings hatte er sie wohl verlegt oder verloren. Das brachte ihn auf die Idee, von seiner Bank nochmals eine Kopie dieser Kontoauszüge zu verlangen. Nach seiner Vorstellung sollte das für ihn kostenlos sein. Denn schließlich steht in Art. 15 DSGVO auch, dass die erste Kopie von Daten kostenlos ist. Erst weitere Kopien dürfen etwas kosten.

Die Bank zeigt sich verschlossen

Die Bank konnte sich mit dieser Idee allerdings nicht anfreunden. Dabei ging es ihr wohl weniger um den einen konkreten Kunden. Vielmehr fürchtete sie, künftig ständig mit solchen Wünschen konfrontiert zu werden. Das wäre in der Summe für sie ziemlich teuer. Deshalb lehnte sie den Wunsch des Kunden ab.

Die Datenschutzaufsicht unterscheidet sehr klug

Der wollte das nicht auf sich beruhen lassen und wandte sich an das Bayerische Landesamt für Datenschutzaufsicht. Es ist in Bayern zuständig für die Datenschutzaufsicht in der Wirtschaft und damit auch für den Datenschutz bei Banken. Das Landesamt entschied über den Wunsch des Kunden im Sinne eines klugen „ja, aber ...“

Eine Auflistung der Kontobewegungen muss die Bank liefern

Das Ja bedeutet: Der Großkunde kann von seiner Bank tatsächlich eine kostenlose Auflistung der Geldbewegungen auf seinem Konto verlangen. Das ergibt sich aus folgenden Überlegungen:

- Bei den Kontobewegungen handelt es sich um personenbezogene Daten. Denn sie beziehen sich auf die Person des Kunden.
- Damit steht dem Bankkunden ein Recht auf Auskunft über diese Kontobewegungen zu.

Das muss kostenlos geschehen

Diese Auskunft muss die Bank grundsätzlich kostenlos erteilen. Etwas anderes würde nur dann gelten, wenn der Kunde ein- und dieselbe Auflistung mehrfach anfordert, ohne dass es dafür einen nachvollziehbaren Grund gibt.

Es gibt keinen Anspruch auf Kopien „alter“ Kontoauszüge

Das Aber folgt jedoch auf dem Fuß: Der Bankkunde kann nicht verlangen, dass die Bank die Auflistung der Kontobewegungen gerade in Form von Kontoauszügen zur Verfügung stellt. Vielmehr kann sie ihm stattdessen etwa eine Tabelle der Kontobewegungen überlassen. Das begründet das Landesamt wie folgt:

- Kontoauszüge sind eine besonders aufbereitete Form von Kontobewegungen.
- Das Auskunftsrecht gibt einem Bankkunden keinen Anspruch darauf, dass er Kontodaten in dieser Weise aufbereitet erhält.
- Die Bank hat ihre Pflicht erfüllt, wenn sie ihm die Daten in irgendeiner geordneten Form zur Verfügung stellt, etwa als Tabelle.
- Alles, was darüber hinausgeht, ist ein Service, der mit dem Auskunftsanspruch nach DSGVO nichts zu tun hat.
- Ob die Bank einen solchen Service überhaupt bietet, ist ebenso ihre Sache wie die Frage, ob sie dafür ein besonderes Entgelt verlangt.

Natürlich gilt dabei: keine Tricks

Allerdings muss alles fair und ohne Tricks ablaufen. Die Bank kann deshalb den Auskunftsanspruch des Kunden zwar auch dadurch erfüllen, dass sie ihm Kopien seiner „alten“ Kontoauszüge zur Verfügung stellt. Dann darf sie dafür allerdings keine Kosten von ihm verlangen. Es ist also zu unterscheiden:

Erteilt die Bank von sich aus Auskunft dadurch, dass sie dem Kunden Kopien von „alten“ Kontoauszügen zur Verfügung stellt, kann sie dafür nichts verlangen.

Will sie jedoch die Auskunft eigentlich in anderer Form erteilen, etwa als Tabelle, und liefert dann auf ausdrücklichen Wunsch des Kunden doch Kopien der früheren Auszüge, kann sie sich das bezahlen lassen.

Der Kunde kann keine Aufbereitung von Daten verlangen

Der Kunde hat also keinen Anspruch auf eine bestimmte Form der Auskunft. Wichtig ist lediglich, dass er eine vollständige Auskunft erhält. Sofern das der Fall ist, kann er keine spezielle Aufbereitung der Daten verlangen.

Smartphone-Apps: Die Suche nach dem Datenschutz



In Zeiten der Pandemie hat die Bedeutung mobiler Geräte und Anwendungen noch weiter zugenommen. Die Zahl der installierten Apps auf Smartphones und Tablets wächst und wächst. Doch wie steht es um den Datenschutz bei den mobilen Anwendungen? Die Antwort fällt nicht immer leicht.

Da gibt es eine App für ...

Handyspiele, Lernprogramme, Büroanwendungen: Im Jahr 2021 gaben die Deutschen so viel Geld für Handy-Apps aus wie noch nie. Insgesamt 2,9 Milliarden Euro Umsatz wurden 2021 mit Smartphone-Programmen generiert, so der Digitalverband Bitkom.

„Das Angebot an Apps wird immer größer – sie ersetzen die Digitalkamera, das Bücherregal, die Spielekonsole“, sagte Dr. Sebastian Klöß, Bereichsleiter für Consumer Technology beim Digitalverband Bitkom. „Gerade in der Corona-Krise haben die Menschen mehr Zeit mit ihrem Smartphone verbracht. Sie haben neue Apps ausprobiert und dabei auch mehr Geld ausgegeben – etwa, um mit kostenpflichtigen Online-Kursen fit zu bleiben, sich mit Spielen die Zeit zu vertreiben oder um neue Sprachen zu lernen.“

Apps gibt es für Geld oder Daten

Wer jetzt denkt, Apps seien doch kostenlos und vielleicht auch deshalb so beliebt, hat zum Teil recht. Die Mehrzahl der mobilen Anwendungen bekommt man tatsächlich, ohne dafür zu bezahlen. Doch ob der Anbieter seine App wirklich ohne Gegenleistung bereitstellt, steht auf einem anderen Blatt.

Viele Apps finanzieren sich über Werbung. Damit die Werbung möglichst relevant und damit erfolgreicher ist, sammeln viele dieser Apps Daten über ihre Nutzerinnen und Nutzer. Daran wäre nichts auszusetzen, wenn denn die Anwender darüber informiert wären und darin eingewilligt hätten.

Tatsächlich sammeln und werten die Apps die Nutzerdaten oftmals aus, ohne eine Information und Zustimmung der Nutzerinnen und Nutzer. Das ist nicht nur bei kostenlosen Apps der Fall. Auch kostenpflichtige Apps können Daten einsammeln, um für ein Zusatzgeschäft zu sorgen.

Wo ist die Datenschutzerklärung?

Ob eine App Daten sammelt, welche Daten sie sammelt und zu welchem Zweck dies geschieht, aber auch wer die Daten des Nutzers oder der Nutzerin erhält, all dies soll in einer Datenschutzerklärung zu finden sein, die vor der Installation der App einzusehen sein muss.

Aber auch nach der Installation der App muss es möglich sein, die Datenschutzerklärung einzusehen. Insbesondere bei einem Update der App kann sich etwas getan haben, das auf den Datenschutz Einfluss hat.

Wer aber bei Apps nach einer Datenschutzerklärung sucht, wird leider nicht immer fündig, im Gegenteil!

Datenschutz hinterfragen: im App-Store und in der App selbst

Ob eine App eine Datenschutzerklärung hat oder nicht, sollte darüber entscheiden, ob man die App überhaupt installiert und nutzt. Die App-Stores wie Google Play für Android-Apps haben in aller Regel einen Link bei der App-Beschreibung, der zur Datenschutzerklärung führt. Leider ist dieser Link nicht so leicht zu finden, zum Beispiel bei den Kontaktdaten des App-Entwicklers.

Noch schwieriger ist es, wenn man die App bereits installiert hat. Hier erscheint es eher wie eine Ausnahme, wenn eine App auch einen Bereich für die Datenschutzerklärung hat. Selbst bei bekannten Apps lässt sich nicht davon ausgehen, dass sie wirklich umfassend über den Datenschutz informieren.

Wer also nicht mit seinen Daten für eine App bezahlen will, ohne genau zu wissen, wer was zu welchem Zweck erfahren wird, sollte auf Apps ohne Datenschutzhinweise verzichten. Tatsächlich wollen viele Apps mehr erfahren, als sie wissen müssten. Das klassische Beispiel sind etwa Apps mit Taschenlampen-Funktion, die auf Standortdaten und Fotos zugreifen wollen. Da sollte einem das Licht aufgehen, dass hier eine App womöglich Nutzerdaten sammeln will.

Wissen Sie, was eine App über Sie weiß? Machen Sie den Test!

Frage: *Kostenpflichtige Apps sammeln keine Nutzerdaten. Stimmt das?*

1. Nein, man kann nicht davon ausgehen, dass der Anbieter einer App, die Geld kostet, keine Zusatzgeschäfte mit Daten machen will.
2. Ja, man bezahlt dann mit Geld und nicht mit seinen Daten..

Lösung: Die Antwort 1. ist (leider) richtig. Selbst kostenpflichtige Apps können Berechtigungen für Datenzugriffe verlangen, die nicht erforderlich sind, und dann Daten über die Nutzerin oder den Nutzer sammeln, um die Daten an Dritte weiterzugeben oder die Daten selbst zu nutzen

Frage: *Apps ohne Datenschutzhinweise werten auch keine Nutzerdaten aus. Stimmt das?*

1. Ja, dann sind bei der App keine personenbezogenen Daten im Spiel.
2. Nein, gerade wenn die Datenschutzerklärung fehlt, kann es sein, dass die App verstärkt Nutzerdaten sammelt und analysiert.

Lösung: Die Antwort 2. ist richtig. Informiert eine App nicht über den Datenschutz, nimmt es der Anbieter offensichtlich nicht sehr genau mit dem Datenschutz. Eine informierte Einwilligung des Nutzers oder der Nutzerin ist nicht möglich. Stattdessen kann es sein, dass unnötige Datenzugriffe erfolgen und Nutzerprofile erzeugt werden, ohne dass der oder die Betroffene eine Ahnung davon hat. Verzichteten Sie daher auf Apps ohne Datenschutzhinweise

Impressum

Redaktion:

Frank Berns, Datenschutzbeauftragter, Geschäftsführer

Anschrift:

Konzept 17 GmbH

Westring 3

24850 Schuby

Amtsgericht Flensburg: HRB 12329

Telefon: 0049 4621 5 30 40 50

E-Mail: mail@konzept17.de