Newsletter Datenschutz

Ausgabe April | 2019

Newsletter der Curacon GmbH Wirtschaftsprüfungsgesellschaft

Liebe Leserin, lieber Leser,

nutzen auch Sie Ihr Smartphone als Navigationsgerät? Dann hält die neue Ausgabe Ihrer Datenschutz-Zeitung vielleicht eine Überraschung für Sie bereit. Denn womöglich haben Sie nicht nur für eine an sich wertlose App bezahlt, sondern Sie sind darüber hinaus Datendieben in die Falle gegangen.

Negative Überraschungen im Datenschutz sollten Sie lieber vermeiden. Deshalb erfahren Sie in dieser Ausgabe zudem, was es mit der gemeinsamen Verantwortlichkeit im Datenschutz auf sich hat, was der Unterschied zwischen Löschen, Vernichten und Einschränken ist und warum ein Lettershop für den Datenschutz ein wichtiges Thema ist. Es ist immer besser, vorher zu wissen, worauf man achten soll, um böse Überraschungen zu verhindern.

Wir wünschen Ihnen viel Spaß beim Lesen!

Ihr Dr. Uwe Günther, Geschäftsführer, Sanovis GmbH, Geschäftsfeldleiter Datenschutz, Curacon GmbH

Ihr Stefan Strüwe, Geschäftsfeldleiter Datenschutz, Curacon GmbH

Navigieren per Smartphone: Praktisch oder riskant?

Das Smartphone hat die bisherigen Navigationsgeräte nahezu verdrängt. Egal ob man beruflich oder privat unterwegs ist – das Smartphone zeigt den Weg. Die Frage ist allerdings, wer alles diesen Weg nachverfolgen kann.

Smartphones als Multifunktionsgeräte

„Das Smartphone ist zu dem Gerät für alle Lebenslagen geworden. Andere Geräte, wie etwa Navigationsgeräte und digitale Kompaktkameras, sind dadurch für viele Nutzer überflüssig geworden", so Dr. Bernhard Rohleder, Hauptgeschäftsführer des Digitalverbands Bitkom.

Möglich geworden ist dies zum einen durch die leistungsstarke Hardware der Smartphones, die in aller Regel auch über GPS-Sensoren verfügen, die früher Navigationsgeräten vorbehalten waren.

Zum anderen sind es die Apps, die Smartphones so vielseitig machen. Apps zur Navigation am Urlaubsort haben drei von zehn Reisenden (29 Prozent) schon einmal eingesetzt, so der Bitkom-Verband. Während der privaten oder beruflichen Autofahrt sind es bereits weitaus mehr. Navigations-Apps gehören zu den besonders beliebten Applikationen für Smartphones, denn sie erscheinen wirklich hilfreich. Und in den meisten Fällen sind sie das auch.

Navi-Apps nicht nur bei Nutzern beliebt

Die hohe Verbreitung von Navigations-Apps hat aber Schattenseiten. Damit ist nicht nur gemeint, dass so manches Werbeunternehmen nur zu gern die Standortdaten der App-Nutzer haben möchte, um die Online-Werbung passender und relevanter zu machen. Zweifellos hat die Werbung für ein Restaurant mehr Aussicht auf Erfolg, wenn man sich in der Nähe befindet.

Neben der Werbeindustrie sind aber auch die Datendiebe an den Navigations-Anwendungen auf Smartphones interessiert. Dabei versuchen sie nicht nur, an die Daten legitimer Navigations-Apps zu gelangen. Sie bringen auch eigene Navi-Apps in Umlauf, leider mit großem Erfolg.

Online-Betrug per Navi-App

Vor einer groß angelegten Betrugsmasche warnte zum Beispiel der IT-Sicherheitsanbieter Eset. Ein Malware-Experte des Anbieters hatte 15 kostenpflichtige gefälschte Navi-Apps im Google Play Store entdeckt. Statt des versprochenen Zusatznutzens boten diese Apps lediglich die Funktionen von Google Maps und zogen dem Anwender dafür Geld aus der Tasche. Bisher wurden die Betrüger-Apps über 50 Millionen Mal installiert. Denn viele Nutzer im Play Store fallen auf die überwiegend guten Bewertungen herein, wie der Security-Anbieter erklärte.

Der Zweck der vermeintlichen Navi-Apps war, Geld zu generieren. Der Anwender zahlte gleich doppelt: mit seinen Nutzerdaten und dem Kaufpreis für eine App, deren Funktionen es bei Google Maps völlig kostenfrei gibt. Ein Teil der beanstandeten Apps verlangte vom Anwender Zugriffsrechte auf die Kontakte und das Telefonbuch – ein deutlicher Hinweis auf Datenschutz-Probleme.

Für den beruflichen wie den privaten Smartphone-Nutzer bedeutet das: Auch kostenpflichtige Apps können zusätzlich Nutzerdaten stehlen. Ohne Schutzsoftware auf dem Smartphone sollte man gar nichts installieren.

Einschaltung eines Lettershops bei persönlicher Werbung

„Bei persönlich adressierter Werbung arbeiten wir immer mit einem Lettershop. Das ist wegen dem Datenschutz." Solche oder ähnliche Sätze hört man in Unternehmen recht oft. Lesen Sie, was es damit auf sich hat und warum man bei Lettershops genau hinschauen sollte.

Bedeutung persönlich adressierter Werbung

Persönlich adressierte Werbung per Brief ist auch in Zeiten des Internets keinesfalls überholt. Je nach Kundengruppe ist sie deutlich erfolgreicher als beispielsweise eine Postwurfsendung an alle Haushalte. Um persönlich adressieren zu können, braucht man Anschriften von Personen, die zur gewünschten Zielgruppe gehören.

Externe Beschaffung von Anschriften

Sind keine solchen Anschriften im Unternehmen vorhanden, müssen sie extern beschafft werden. Dabei sind im Prinzip zwei Wege denkbar:

- Weg Nr. 1: Das Unternehmen kauft die Adressen bei einem Adresshändler und bekommt sie tatsächlich in die Hand. Dann kann es sie dauerhaft nutzen.
- Weg Nr. 2: Das Unternehmen kauft lediglich das Recht, bestimmte Adressen einmal oder auch mehrmals zu verwenden, ausgehändigt werden ihm diese Adressen jedoch nicht. Sie bleiben vielmehr bei dem Adresshändler, der über die Adressen verfügt.

Bei beiden Wegen können sogenannte Lettershops als Dienstleister ins Spiel kommen. Man versteht dann darunter jedoch sehr verschiedene Dinge.

Einschaltung eines Lettershops durch den Käufer der Anschriften

Bei Weg Nr. 1 beauftragt das Unternehmen, das die Adressen gekauft hat, einen Lettershop. Er hat die Aufgabe, für den Versand des Werbematerials zu sorgen. Dazu steckt er es in Umschläge und versieht die Umschläge mit Adressen. Das Unternehmen stellt ihm dafür die gekauften Adressen zur Verfügung.

Rechtlich gesehen handelt es sich um eine Auftragsverarbeitung für das Unternehmen, das die Adressen gekauft hat. Zwischen diesem Unternehmen und dem Lettershop ist deshalb ein Vertrag über Auftragsverarbeitung erforderlich. Der Adresshändler spielt dabei keine Rolle.

Einschaltung eines Lettershops durch den Adresshändler

Bei Weg Nr. 2 wird es etwas komplizierter. Die Ausgangslage stellt sich wie folgt dar: Das Unternehmen, das für die Adressen bezahlt hat, soll sie nutzen können, bekommt sie jedoch nicht in die Hand. Der Adresshändler wiederum will die Nutzung der Adressen zulassen, sie aber nicht aus der Hand geben.

Die Lösung des Problems: Es wird ein Lettershop als eine Art neutraler Dritter eingeschaltet. Der Adresshändler stellt dem Lettershop die Adressen zur Verfügung. Das Unternehmen, das werben möchte, liefert beim Lettershop das Werbematerial an. Aufgabe des Lettershops ist es, Werbematerial und Adressen zusammenzuführen und dann die Werbebriefe zu versenden.

Deutlich andere Funktion

Schon auf den ersten Blick wird deutlich, dass der Lettershop hier eine andere Funktion hat als bei Weg Nr. 1. Datenschutzrechtlich ist der Lettershop als ein Auftragsverarbeiter anzusehen, der für den Adresshändler handelt. Denn von ihm erhält er die personenbezogenen Adressen. Das werbende Unternehmen hat damit nichts zu tun. Deshalb ist in diesem Fall ein Vertrag über Auftragsverarbeitung zwischen dem Adresshändler und dem Lettershop erforderlich.

Rechtliche Bedeutung der Unterscheidung

Bei diesen Unterscheidungen geht es nicht nur um juristische Spitzfindigkeiten. Wer einen Auftragsverarbeiter einschaltet, haftet normalerweise auch für ihn, sollte der Auftragsverarbeiter Datenschutzverstöße begehen. Deshalb ist es keinesfalls gleichgültig, auf wessen Seite ein Auftragsverarbeiter steht.

Keine Begriffsdefinition im Gesetz

Gesetzlich definiert ist der Begriff „Lettershop" übrigens weder im Datenschutzrecht noch sonst in irgendeinem Gesetz. Deshalb sollte man immer genau nachfragen, was mit diesem Begriff jeweils gemeint ist. Wie die Verträge gestaltet werden, muss dann dazu passen. Mit dem Schlagwort für sich allein ist nichts gewonnen.

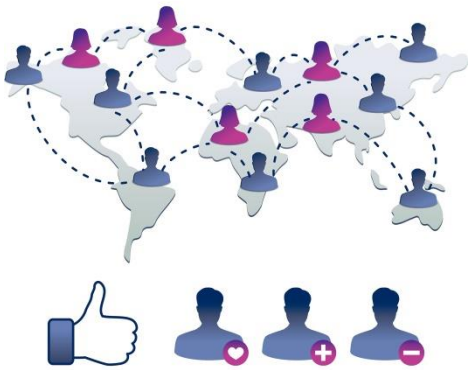
Ziele außerhalb des Datenschutzes

Aus der Sicht des Datenschutzes ist der Einsatz eines Lettershops weder gut noch böse. Wenn es aus der Sicht eines Unternehmens sinnvoll ist, kann es Lettershops beauftragen. Wichtig ist dabei nur, seine Rolle klar zu definieren und die vertraglichen Vereinbarungen danach auszurichten. Dann gibt es auch vom Datenschutz her keine Probleme.

Dass ein Lettershop wegen des Datenschutzes eingesetzt werden müsste, stimmt nicht. Es geht vielmehr vor allem darum, dass er die Adressierung und den Versand besonders professionell beherrscht. Und beim oben geschilderten Weg Nr. 2 (keine Aushändigung der Adressen durch den Adresshändler) möchte der Adresshändler die Adressen schlicht stets unter seiner Kontrolle haben.

Gemeinsame Verantwortung von Unternehmen im Datenschutz

Manchmal wirken mehrere Unternehmen bei der Verarbeitung von personenbezogenen Daten zusammen. Klassisches Beispiel: Um einen Vertrag zu erfüllen, werden Subunternehmer eingeschaltet. Wer trägt dann datenschutzrechtlich gesehen die Verantwortung für die Daten? Neue Entscheidungen des Europäischen Gerichtshofs führen dazu, dass Unternehmen hier genauer hinschauen müssen. Dabei stellen sich Fragen, die auf den ersten Blick merkwürdig wirken. Sie richten sich an die Fachabteilungen in den Unternehmen. Deshalb sollten Sie darauf vorbereitet sein.



Eine absurde Ausgangslage?

Ein Unternehmen hat auf bestimmte personenbezogene Daten überhaupt keinen Zugriff. Dennoch soll es datenschutzrechtlich dafür verantwortlich sein, was ein anderes Unternehmen mit diesen Daten tut. Sie meinen, das könne überhaupt nicht sein? Dann unterschätzen Sie die Kreativität des Europäischen Gerichtshofs. Denn genauso hat er gleich in zwei Fällen entschieden. Beim ersten Fall ging es um Facebook, beim zweiten um die Zeugen Jehovas. Aus beiden Fällen lassen sich allgemeine Regeln ableiten, die in den Alltag zahlreicher Unternehmen hineinwirken.

Fanpages bei Facebook

Der erste Fall befasste sich mit dem Thema „Fanpages bei Facebook". Dabei ging es um Folgendes: Fanpages sind Benutzerkonten, die Unternehmen (aber auch Privatpersonen) bei Facebook einrichten können. Dazu muss sich das Unternehmen als Fanpage-Anbieter bei Facebook registrieren. Ist das geschehen, dann hat der Anbieter eine Plattform, um sich den Nutzern von Facebook, aber auch allen sonstigen Personen, die die Fanpage besuchen, zu präsentieren. Der Betreiber einer Fanpage kann mithilfe der Funktion „Facebook Insight" anonymisierte statistische Daten zu den Nutzern dieser Seiten erhalten.

Rein anonyme Auswertungen

Diese Funktion stellt Facebook kostenfrei zur Verfügung. Auf diese Funktion zu verzichten, ist nicht möglich. Die Daten der Nutzer sammelt Facebook mithilfe sogenannter Cookies. Wer eine Fanpage einrichtet, erhält nur Auswertungen dieser Daten, nicht aber die Daten selbst. Er erfährt also viel über die Besucher der Fanpage allgemein, aber nichts über den einzelnen Besucher konkret.

Dennoch: Verantwortung des Auftraggebers

Das hilft freilich den Betreibern von Fanpages nichts. Der Europäische Gerichtshof stellte vielmehr fest, dass sie zusammen mit Facebook datenschutzrechtlich verantwortlich sind. Dass ihnen Facebook nur anonyme Statistiken überlässt, nicht jedoch die einzelnen personenbezogenen Daten, erklärte das Gericht für irrelevant. Denn immerhin würden sie durch das Einrichten ihrer Fanpage an der Datensammlung mitwirken.

Zeugen Jehovas – ein keineswegs exotischer Fall

Ähnlich hart entschied der Gerichtshof im Fall der Zeugen Jehovas. Zwar konnten die Zeugen Jehovas glaubhaft machen, dass lediglich die einzelnen Missionare dieser Kirche Daten festhalten – etwa nach Missionsgesprächen an der Haustür. Die Kirchenzentrale erhält diese Daten nicht. Weil die Kirche ihren Mitgliedern jedoch Tipps dafür gibt, welche Daten sie möglichst festhalten sollen, ging der Gerichtshof auch hier von einer gemeinsamen Verantwortlichkeit aus. Sie besteht zwischen der Kirche Zeugen Jehovas einerseits und den Missionaren dieser Kirche andererseits.

Allgemeine Lehren aus dem Fall

Schon kurzes Überlegen zeigt: Der entscheidende Punkt ist hier nicht, dass es um eine religiöse Missionstätigkeit geht. Das spielt überhaupt keine Rolle. Entscheidend ist vielmehr, dass die Kirche für das verantwortlich ist, was ihre Mitglieder tun. Und zwar obwohl sie selbst keinerlei personenbezogene Daten in die Hände bekommt.

Verantwortlichkeit kann teuer kommen

Sind das alles nur rechtliche Spitzfindigkeiten ohne praktische Auswirkung? Leider nein! Denn wer gemeinsam für etwas verantwortlich ist, haftet auch gemeinsam. Dies kann bei Datenpannen bis hin zu erheblichen Schadenersatzzahlungen gehen. Wohlgemerkt für Pannen mit Daten, auf die man selbst überhaupt keinen Zugriff hatte oder hat.

Helfen Sie durch sorgfältige Antworten

Wundern Sie sich also nicht, falls Sie einmal solche Fragen beantworten müssen:

- Machen Sie Geschäftspartnern Vorgaben dafür, welche Daten sie festhalten müssen?
- Erhalten Sie Auswertungen von Daten, ohne dass Sie auf die Daten selbst Zugriff haben?

Auch das hat dann etwas mit Datenschutz zu tun. Aber es geht dabei nicht darum, etwas zu verbieten. Vielmehr sollen Haftungsrisiken für das Unternehmen vermieden werden. Bitte wirken Sie daran mit, indem Sie die Fragen sorgfältig beantworten.

Impressum

Redaktion
Dr. Uwe Günther
Sanovis GmbH

Stefan Strüwe, RA
CURACON GmbH
Wirtschaftsprüfungsgesellschaft

Anschrift
Richard-Strauss-Str. 69
81679 München
Telefon: 089 / 99 27 579 22
E-Mail: Uwe.Guenther@Sanovis.com

Am Mittelhafen 14
48155 Münster
Telefon: 02 51 / 92 208 209
E-Mail: Stefan.Struewe@curacon.de

Einschränken, Löschen oder Vernichten: Was sind die Unterschiede?

Reicht es, Daten zu löschen, oder muss man gleich das ganze Speichermedium vernichten? Was hat es mit der Einschränkung der Verarbeitung auf sich? Verschaffen Sie sich den Durchblick!

Das Problem mit dem Löschen

Warum soll ich die Daten denn löschen, wir haben doch genug Speicherplatz, und vielleicht kann man die Daten später nochmals gebrauchen, so denken Sie vielleicht manchmal, wenn Sie Daten früherer Kunden löschen sollen. Die Antwort ist schnell gegeben: Die früheren Kunden haben ein Recht darauf, so will es die Datenschutz-Grundverordnung.

Das Löschen ist aber auch aus Unternehmenssicht sinnvoll: Gelöschte Daten lassen sich nicht mehr stehlen und missbrauchen. Datenlöschung ist Datenschutz, spart Speicherkosten und vereinfacht die Datenverwaltung. Wichtig ist es allerdings, dass die Daten auch sicher und vollständig gelöscht werden.

Wenn das Löschen nicht möglich ist

Was aber ist, wenn sich die Daten nicht löschen lassen, wenn sie sich zum Beispiel auf einem Speichermedium befinden, von dem man sie nicht löschen kann, zum Beispiel einer einmal gebrannten CD, die sich nicht verändern lässt? Muss man dann nicht löschen?

Aus Sicht des Datenschutzes müssen Daten gelöscht werden, wenn die Löschverpflichtung nach Datenschutz-Grundverordnung eintritt und keine gesetzliche oder vertragliche Pflicht zur Aufbewahrung mehr besteht. Ist es nicht möglich, die Daten zu löschen, steht die Vernichtung des Speichermediums an.

„Vernichten" bedeutet dabei „völlige Zerstörung" und wird unter anderem in Verbindung mit der Entsorgung von Akten und anderen Papierdokumenten als Begriff genutzt. Für den Datenschutz sind Papierdokumente Datenträger, wenn sich auf den Dokumenten personenbezogene Daten befinden. Vernichtet oder zerstört werden nicht nur Papierdokumente, sondern auch Speichermedien wie CDs. Dafür werden spezielle Werkzeuge und Verfahren genutzt.

Wissen Sie, wie und durch wen die Datenträger korrekt vernichtet werden? Wenn nicht, fragen Sie bitte nach!

Einschränkung: die große Unbekannte

Während man sich unter „Löschen" und „Vernichten" noch etwas vorstellen kann, scheint die sogenannte Einschränkung der Verarbeitung personenbezogener Daten etwas Komisches zu sein. Darf man die Daten etwa nur teilweise verarbeiten? Nein, Einschränkung bedeutet im Datenschutz: gespeicherte personenbezogene Daten zu markieren mit dem Ziel, ihre künftige Verarbeitung einzuschränken. Die betroffene Person kann in bestimmten Fällen die Einschränkung der Verarbeitung verlangen, das heißt, dass das Unternehmen die Daten zwar nicht löscht, sie aber auch nicht mehr anderweitig verarbeiten darf.

Das lässt sich beispielsweise dadurch erreichen, dass Daten für Nutzer gesperrt oder von einer Website entfernt werden.

Eine Einschränkung der Verarbeitung können Unternehmen zum Beispiel dann geltend machen, wenn das Recht oder die Pflicht zur Löschung bestimmter Daten besteht, der Löschung aber Interessen der betroffenen Person entgegenstehen, und andererseits in Fällen, in denen die Überprüfung von Löschansprüchen eine gewisse Zeit erfordert.

Man kann sich dann die Einschränkung der Verarbeitung vorstellen als Vorbereitung einer anstehenden Löschung, um in der Zwischenzeit eine Verarbeitung zu verhindern.

Löschen, Vernichten oder Einschränken

Vernichten, Löschen und Einschränken dienen also jeweils dem Ziel, die personenbezogenen Daten zum Beispiel früherer Kunden vor Verarbeitung zu schützen, weil es keine Einwilligung mehr gibt, weil die Daten falsch sind oder weil der Verarbeitungszweck erfüllt ist und keine Aufbewahrung mehr stattfinden muss. Dabei muss man beachten, wann Unternehmen Daten löschen, wann sie einschränken und wann vernichten müssen.

Kennen Sie den Unterschied von Löschen, Vernichten und Einschränken?

Machen Sie den Test!

Frage: ***Kann ein Datenträger nicht gelöscht werden, muss er sofort vernichtet werden. Stimmt das?***

a. Nein, denn vielleicht hat der Betroffene ein Interesse daran, dass die Daten nicht gelöscht werden, oder der Löschanspruch muss erst noch geklärt werden.

b. Ja, klappt das Löschen nicht, zerstört man umgehend das Speichermedium.

Lösung: Die Antwort a. ist richtig. Denn vor der Vernichtung der Datenträger und damit der endgültigen Zerstörung der Daten müssen Unternehmen erst den Löschanspruch und das Interesse des Betroffenen prüfen. Die Verarbeitung der Daten wird dann so lange eingeschränkt, bis der Löschanspruch geprüft wurde.

Frage: ***Die Einschränkung der Verarbeitung kann das Löschen der Daten dauerhaft ersetzen. Stimmt das?***

a. Ja, denn dann können die Daten ja nicht mehr verarbeitet werden.

b. Nein, Löschen und Einschränken sind unterschiedliche Rechte, Unternehmen haben nicht die Auswahl.

Lösung: Die Antwort b. ist richtig. Die Einschränkung ist nicht gedacht als Dauerlösung und als Ersatz für das Löschen. Stattdessen findet zum Beispiel eine Einschränkung statt, wenn die Verarbeitung unrechtmäßig ist, die betroffene Person die Löschung der personenbezogenen Daten aber ablehnt, Löschansprüche überprüft werden müssen oder die betroffene Person die Daten noch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt.