Newsletter Datenschutz

Ausgabe Juni | 2019

CURACON SANOVIS

SICHERHEIT GEBEN. LÖSUNGEN BIETEN. CONSULTING WITH CARE.

Newsletter der Curacon GmbH Wirtschaftsprüfungsgesellschaft

Liebe Leserin, lieber Leser,

Politik, Recht und IT haben gemeinsam, dass sie schnellen Änderungen unterworfen sind, die auch Auswirkungen auf den Datenschutz haben. In dieser Ausgabe erfahren Sie, welche Folgen der Austritt von Großbritannien aus der EU, auch Brexit genannt, für den Datenschutz haben kann. Ebenso lesen Sie, worauf Sie achten müssen, wenn sie einen Cloud-Dienst aus den USA verwenden.

Zum Betriebssystem Windows 10 gibt es weitere Datenschutz-Erkenntnisse, die Sie als möglicher privater oder beruflicher Nutzer kennen sollten. Doch nicht nur neue Technologien und politische Entwicklungen berühren den Datenschutz. Bereits das Versenden von E-Mails kann zu einem Datenschutz-Problem werden, wenn es zu Fehlsendungen kommt.

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

Wie steht es um den Datenschutz bei Cloud-Diensten aus den USA?

Die führenden Cloud-Anbieter AWS, Google und Microsoft stammen aus den USA. Es stellt sich daher die Frage, wie sich der Datenschutz in diesen Clouds gewährleisten lässt. Aufsichtsbehörden haben Hinweise dazu gegeben.

Das Trio der Public-Cloud-Anbieter

Geht es um den Einsatz von öffentlichen, gemeinsam genutzten Cloud-Diensten (Public Cloud), fällt die Wahl meist auf einen der drei großen US-Anbieter. Laut der aktuellen RightScale-Studie „State of the Cloud Report" setzen 61 Prozent der weltweit befragten Firmen auf Amazon Web Services (AWS), 52 Prozent auf Microsoft Azure und 19 Prozent auf die Google Cloud. Offensichtlich nutzen Unternehmen sogar mehr als einen Cloud-Dienst aus den USA. Von den Cloud-Diensten versprechen sich Unternehmen eine flexible Nutzung von IT-Diensten, Kostenvorteile im Vergleich zur internen IT und weniger Aufwand für das eigene IT-Personal.

Doch Flexibilität, Kostenreduktion und ein geringerer Aufwand in der IT-Abteilung sind nicht alles, um was es gehen sollte. Denn bei Cloud-Diensten aus den USA kann man nicht einfach davon ausgehen, dass die Forderungen aus der Datenschutz-Grundverordnung (DSGVO) der EU erfüllt sind.

Aufsichtsbehörden fordern ein angemessenes Datenschutzniveau

Bevor ein deutsches Unternehmen einen Cloud-Dienst aus den USA nutzt, muss es sicherstellen, dass der Anbieter die DSGVO-Anforderungen erfüllt. Da nicht nur die IT-Abteilung, sondern vielfach auch die Fachbereiche und einzelne Nutzer zu Cloud-Services greifen, sollte jeder potenzielle Cloud-Nutzer daran denken, das Datenschutzniveau zu hinterfragen.

Beispiel: Vorgaben für Microsoft Azure

Eine Aufsichtsbehörde für den Datenschutz hat kürzlich Hinweise dazu veröffentlicht, worauf im Fall von Microsoft Azure zu achten ist. Das lässt sich auch als Beispiel für andere Cloud-Dienste aus den USA nutzen.

Als Voraussetzungen für einen datenschutzgerechten Einsatz nennt die Aufsicht: eine wirksame Zusatzvereinbarung, die die Vorgaben für eine Auftragsverarbeitung (Artikel 28 DSGVO) enthält, eine Verschlüsselung der Daten unabhängig vom Cloud-Anbieter (HYOK, Hold Your Own Key, Hoheit über den Schlüssel beim Nutzer selbst) und eine Möglichkeit, den Versand von Nutzungsdaten (Telemetriedaten) an den Cloud-Anbieter zu unterbinden. Vor dem Einsatz eines Cloud-Dienstes aus den USA ist zudem eine Risikoanalyse (Datenschutz-Folgenabschätzung, Artikel 35 DSGVO) nötig. Ist es dem Unternehmen oder Nutzer nicht möglich, diese Voraussetzungen zu gewährleisten, empfiehlt es sich aus Sicht des Datenschutzes, auf entsprechende Cloud-Dienste aus den USA zu verzichten.

Wichtig ist es nun, auf weitere Hinweise der Aufsichtsbehörden zu achten und in Zukunft solche Cloud-Dienste zu verwenden, die ein Datenschutzzertifikat vorweisen können, das der DSGVO entspricht. Hier wird es in naher Zukunft zahlreiche Cloud-Angebote geben.

CURACON SANOVIS
SICHERHEIT GEBEN. LÖSUNGEN BIETEN. CONSULTING WITH CARE.

Brexit und Datenschutz

Geht Großbritannien jetzt, oder bleibt es doch in der Europäischen Union (EU)? Im Augenblick weiß das niemand. Und genau das macht Schwierigkeiten – auch im Datenschutz. Jedes Unternehmen muss damit irgendwie umgehen. Ein Patentrezept gibt es nicht.

Aufgeschoben, nicht aufgehoben

Im Augenblick ist der Brexit aufgeschoben. Der 31.10.2019 wurde Mitte April zwischen Großbritannien und den anderen Mitgliedstaaten der Europäischen Union als spätester Austrittstermin vereinbart. Wohlgemerkt: als spätester Termin. Sollten sich Großbritannien und die EU schneller einigen, bleibt ein Austritt auch schon vorher möglich. Damit ist nach wie vor alles offen. Genau dies macht Unternehmen eine Vorausplanung so gut wie unmöglich. Je nach weiterer Entwicklung können daher kurzfristige Reaktionen erforderlich sein.

Variante 1: geordneter Brexit

Für alle Beteiligten am besten wäre es, wenn es noch zu einem Abkommen über einen geordneten Brexit kommt. „Geordnet" würde dabei heißen, dass es eine einvernehmliche Vereinbarung über den Brexit gibt. In einem solchen Vertrag würden sich Großbritannien und die EU dann auch darüber verständigen, was im Datenschutz gilt. Vermutlich würde Großbritannien zusagen, auch künftig die Datenschutz-Grundverordnung (DSGVO) einzuhalten. Die EU wiederum würde erklären, dass damit im Datenschutz alles so weiterlaufen kann wie bisher gewohnt.

Bequemes Ergebnis

Das würde bedeuten: Der Austausch personenbezogener Daten mit Unternehmen in Großbritannien ließe sich einfach wie gewohnt fortführen. Besonderer Handlungsbedarf für Unternehmen bestünde nicht.

Variante 2: harter Brexit

Es kann aber auch ganz anders kommen. Angenommen, Großbritannien und die EU trennen sich im Streit und können sich nicht auf ein Abkommen einigen. Dann würde Großbritannien am 31.10.2019 automatisch aus der EU ausscheiden. Es wäre dann rechtlich so zu behandeln wie jeder andere Staat außerhalb der Europäischen Union. In der Sprache des EU-Rechts wäre es damit ein Drittstaat, also schlicht ein Nicht-Mitglied.

Gravierende Folgen

Das hätte gerade im Datenschutz gravierende Folgen. Unternehmen dürften personenbezogene Daten dann nur noch unter den Voraussetzungen nach Großbritannien übermitteln, die für eine Übermittlung in jeden anderen Drittstaat gelten, der nie EU-Mitglied war. Dies wäre ausgesprochen misslich. Denn die wirtschaftlichen Verflechtungen mit Großbritannien sind äußerst vielfältig und eng. Das ist eine Folge der jahrzehntelangen Teilnahme Großbritanniens am Binnenmarkt.

Situation betroffener Unternehmen

Innerhalb der gesamten EU dürfen personenbezogene Daten frei übermittelt werden, solange die Vorgaben der DSGVO eingehalten sind. Eine Übermittlung in einen Drittstaat setzt dagegen eine besondere Rechtsgrundlage voraus. Es ist Sache des Unternehmens, eine solche Rechtsgrundlage nachzuweisen. Die Folge: Für jede Datenübermittlung nach Großbritannien müsste geklärt werden, ob eine solche Rechtsgrundlage besteht. Welcher Aufwand damit verbunden ist, kann man sich leicht ausmalen.

Er würde vor allem die Abteilungen in den Unternehmen treffen, die solche Übermittlungen durchführen. Denn nur sie verfügen über die nötigen Informationen zu deren genauem Ablauf.

„Standarddatenschutzklauseln" als Hilfe

Die meisten Unternehmen planen, bei einem harten Brexit Standarddatenschutzklauseln einzusetzen. Das sind offizielle Muster der EU für vertragliche Regelungen zum Datenschutz. Sie können bei der Datenübermittlung in Drittstaaten mit dem Vertragspartner im Drittstaat vereinbart werden. Der Vorteil dieser Klauseln: Sie lassen sich ohne besondere Genehmigung verwenden. Außerdem stehen sie in allen Amtssprachen der EU kostenlos zur Verfügung. Ihr Nachteil: Es kommt zu viel Schreibkram, der bisher völlig entbehrlich war.

Manche Unternehmen haben mit ihren Partnern in Großbritannien vorsorglich bereits entsprechende Vereinbarungen getroffen. Andere Unternehmen warten ab. Sie hoffen darauf, diesen Aufwand doch noch vermeiden zu können. Was der bessere Weg war, wird man erst im Nachhinein wissen, also zu spät.

Übersichten zur aktuellen Situation

Nahezu alle Unternehmen haben aus Vorsicht Übersichten dazu angefertigt, welche Datenübermittlungen nach Großbritannien stattfinden. Wer es noch nicht getan hat, wird dieses Thema in nächster Zeit angehen. Denn nur so ist es möglich, bei Bedarf kurzfristig zu handeln. Die Zuverlässigkeit solcher Übersichten steht und fällt mit der sorgfältigen Zuarbeit aus den Fachabteilungen.

Die Begeisterung über den Aufwand hält sich verständlicherweise in Grenzen. Er ist jedoch notwendig. Denn sonst drohen bei einem ungeordneten Brexit ernsthafte Beeinträchtigungen der Tagesarbeit im Unternehmen.

Datenpannen durch Fehlversendungen

Eine E-Mail mit personenbezogenen Daten geht per cc versehentlich an Adressaten, die sie gar nicht erhalten sollten. Personalunterlagen werden per Post an den falschen Herrn Meier geschickt. Alles nicht so schlimm? Eine kurze freundliche Entschuldigung, und alles ist wieder gut? So einfach ist es leider nicht!

Pflicht, Datenpannen zu melden

Die Datenschutz-Grundverordnung (DSGVO) enthält eine Verpflichtung, Verletzungen des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde für den Datenschutz zu melden. Dies muss im Normalfall binnen 72 Stunden geschehen. Eine Ausnahme hiervon gilt nur dann, wenn voraussichtlich nicht mit Risiken für die betroffenen Personen zu rechnen ist. So regelt es Art. 33 Abs. 1 DSGVO.

Jedes Unternehmen muss sich so organisieren, dass es Datenpannen tatsächlich bemerkt. Anders gesagt: Es muss seine Mitarbeiterinnen und Mitarbeiter dazu verpflichten, Datenpannen auch zu melden.

Vorbeugende Maßnahmen

Noch besser ist es natürlich, wenn solche Pannen erst gar nicht vorkommen. Die häufigste Art von Pannen sind Fehlversendungen. Das zeigen die Statistiken der Aufsichtsbehörden. Sie betreffen sowohl klassische Briefsendungen als auch E-Mails. Die Gründe sind jeweils unterschiedlich.

Pannen bei Briefsendungen

Bei Briefsendungen ist es schlicht so, dass vor allem jüngeren Mitarbeiterinnen und Mitarbeitern die Übung im Umgang mit Briefen fehlt. Privat schreiben sie kaum welche. Und im Unternehmen sind Briefe tendenziell ebenfalls seltener geworden.

Der Klassiker in diesem Bereich: Es müssen Unterlagen an eine größere Zahl von Adressaten verschickt werden. Auf den Unterlagen steht jeweils die Anschrift des Adressaten, und zwar fehlerfrei. Die Umschläge werden getrennt davon mit der jeweiligen Anschrift versehen. Beim Zusammenführen von Umschlägen und Unterlagen passieren dann die Fehler. Die Unterlagen kommen jeweils in den falschen Umschlag. Das geschieht besonders oft, wenn Praktikanten oder andere wenig geübte Personen damit beauftragt werden.

Schnell stellt sich dann heraus, dass auch solche scheinbar einfachen Arbeiten eben doch nicht „jeder kann".

Fensterumschläge als Lösung?

Manche Aufsichtsbehörden empfehlen inzwischen, in solchen Fällen Fensterumschläge zu verwenden. Dann ist es nicht mehr nötig, die Umschläge gesondert zu beschriften. Vielmehr wird die entsprechende Unterlage so in den Umschlag hineingesteckt, dass die Anschrift im Brieffenster erscheint. Das ist an sich keine schlechte Idee. Freilich kann dabei ein anderes Problem auftauchen. Immer wieder beginnt nämlich der Text auf einer Unterlage so nah an der Anschrift, dass Teile des Textes im Brieffenster zu sehen sind. Auch wenn es sich banal anhört, ist hier also genaues Falten des Papiers gefragt. Das verlangt ebenfalls Übung.

Vier-Augen-Prinzip

Eine andere Möglichkeit wäre, nach dem Vier-Augen-Prinzip vorzugehen. Das bedeutet allerdings, dass jeder Brief von zwei Mitarbeitern in die Hand genommen werden muss. Dieser Aufwand ist oft schlicht zu groß.

Pannen bei E-Mails

Klassische Datenpannen beim Versand von E-Mails ist die versehentliche Nutzung der cc-Funktion anstelle der bcc-Funktion, um ein und dieselbe Mail an eine größere Zahl Adressaten zu schicken. Sie wissen nicht, was der Unterschied ist? Dann sollten Sie offen gesagt die Finger davon lassen, mit diesen Funktionen zu arbeiten.

Nur kurz zur Erinnerung: Bei der bcc-Funktion sieht ein Adressat die E-Mailadressen der anderen Adressaten nicht, bei der cc-Funktion dagegen schon. Auf diese Weise ist dann schnell einmal eine komplette Kundenliste offengelegt. Dadurch kann dann ein Problem entstehen, das weit über den Datenschutz hinausreicht.

Die Funktion „an alle"

Eine ausgesprochen tückische Funktion ist auch die Funktion „an alle". Mit „alle" sind dabei dann beispielsweise sämtliche Mitarbeiter eines Unternehmens gemeint, die ein E-Mailsystem benutzen. Das können Tausende von E-Mailadressen sein.

Viele Unternehmen behalten die Nutzung dieser Funktion deshalb bestimmten Personen oder Funktionseinheiten vor (beispielsweise der Pforte, wenn sie etwa in einem Notfall eine Warnung verschicken muss, und der Firmenleitung, wenn es zum Beispiel um Weihnachtsgrüße an alle geht). Solche Beschränkungen sind weder Schikane noch Misstrauen. Sie verhindern im Gegenteil Pannen größerer Art.

Wegducken hilft nicht!

In jedem Fall gilt: Sollte es zu einer Versendungspanne kommen, muss dies sofort dem Vorgesetzten gemeldet werden. Denn nur so kann das Unternehmen seine Meldepflicht gegenüber der Datenschutzaufsicht erfüllen.

Impressum

Redaktion
Dr. Uwe Günther
Sanovis GmbH

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

Stefan Strüwe, RA
CURACON GmbH
Wirtschaftsprüfungsgesellschaft

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

Windows 10: Immer auf Sendung?

Das Microsoft-Betriebssystem Windows 10 ist in Unternehmen und Privathaushalten weit verbreitet. IT-Sicherheitsbehörden und Datenschützer prüfen nun ausführlich den Umgang von Windows 10 mit Nutzerdaten. Erste Prüfungsergebnisse liegen bereits vor.

Betriebssysteme sind entscheidend für die Datensicherheit

Unter der Software, die auf PCs, Notebooks und Tablets installiert ist, kommt den Betriebssystemen eine große Bedeutung zu. Auch wenn jede eingesetzte Software datenschutzkonform sein sollte – bei Betriebssystemen kommt es ganz besonders darauf an. Denn sie bilden die Basis für alle anderen installierten Anwendungen.

Das aktuelle Betriebssystem von Microsoft namens Windows 10 ist auf vielen neuen Bürorechnern zu finden, ältere Rechner wurden oftmals, soweit möglich, bereits auf Windows 10 umgestellt. Entsprechend betrifft die Frage viele Nutzer und Unternehmen, wie es denn Windows 10 mit dem Datenschutz hält.

IT-Sicherheitsbehörde überprüft Sicherheit von Windows 10

Die nationale IT-Sicherheitsbehörde BSI (Abk. für „Bundesamt für Sicherheit in der Informationstechnik") hat sich der Frage angenommen, was Windows 10 mit den Nutzer- und Nutzungsdaten macht. Ein erstes Ergebnis des BSI: Das Betriebssystem Windows 10 sendet umfangreiche System- und Nutzungsinformationen an Microsoft. Dass Windows diese sogenannten Telemetriedaten erfasst und überträgt, lässt sich zwar technisch unterbinden. Für Anwender ist das aber nur schwer umzusetzen.

Zudem haben auf dem Rechner installierte Anwendungen wie Microsoft Office die Möglichkeit, auch ohne den zentralen Dienst des Betriebssystems Telemetriedaten zu erfassen und an den Hersteller zu versenden. Beispiele für Telemetriedaten sind Informationen zur Häufigkeit, mit der der Nutzer Funktionen von Windows, Microsoft-Anwendungen und Hardware-Funktionen einsetzt.

„Mehr als ein Drittel der Computernutzer weltweit setzt Windows 10 ein, Tendenz steigend. Daher prüfen wir das Betriebssystem auf Herz und Nieren und leiten daraus im Sinne eines digitalen Verbraucherschutzes konkrete Empfehlungen ab, mit denen die Digitalisierung ein Stück sicherer wird", erklärte Arne Schönbohm, Präsident des BSI.

Datenschutzaufsicht kündigt weitere Prüfungen an

Die Datenschutz-Grundverordnung (DSGVO) verlangt von Unternehmen beim Einsatz von Windows 10, die datenschutzkonforme Verarbeitung personenbezogener Daten sicherzustellen. Dies bedeutet für die Verantwortlichen derzeit einen erheblichen Aufwand, so die Aufsichtsbehörden für den Datenschutz. Deshalb wollen die Datenschutzbehörden nun eine weitergehende Überprüfung des Betriebssystems vornehmen.

Dabei weisen die Datenschützer zum Beispiel auf Folgendes hin: Jedes Update (insbesondere die Funktionsupdates) kann dazu führen, dass sich bei Windows 10 sowohl Konfigurationseinstellungen als auch der Funktionsumfang verändern. Dies führt dazu, dass jeweils ein neues Produkt vorliegt, dessen Einsatz Unternehmen erneut auf die datenschutzrechtliche Zulässigkeit prüfen müssen.

Unternehmen müssen am Ball bleiben

Für berufliche und private Nutzer bedeutet das, dass es nicht ausreicht, möglichst strenge Datenschutz-Einstellungen bei Windows 10 vorzunehmen. Der Datenschutz bei Windows 10 muss als sich ständig entwickelndes Thema verstanden werden.

Es ist wichtig, sich über das richtige Vorgehen bei den Datenschutz-Einstellungen von Windows 10 regelmäßig zu informieren. Denn noch gibt es keine abschließende Einstellung, die mit Sicherheit für den notwendigen Datenschutz sorgt.

Kümmern Sie sich richtig um den Datenschutz bei Windows 10?

Machen Sie den Test!

Frage: ***Windows 10 bietet umfangreiche Datenschutz-Optionen. Man muss nur die strengste Einstellung auswählen, dann passt der Datenschutz. Stimmt das?***

a. Nein. Einstellungen, die ein normaler Nutzer vornehmen kann, reichen bisher nicht aus, um zum Beispiel den Versand von Nutzungsdaten an Microsoft zu unterbinden.

b. Ja. Wenn die Datenschutz-Optionen richtig ausgewählt sind, ist Windows 10 automatisch konform mit der Datenschutz-Grundverordnung.

Lösung: Die Antwort a. ist richtig. Denn bisher gibt es von Microsoft keine einfach zu bedienende Datenschutz-Funktion, mit der sich zum Beispiel der Versand der sogenannten Telemetriedaten abstellen lassen würde.

Frage: ***Ein Betriebssystem wie Windows 10 muss einmal bei der Installation auf den richtigen Datenschutz geprüft werden. Stimmt das?***

a. Ja, eine Prüfung gleich nach der Installation ist ausreichend.

b. Nein. Zum einen sollte es vor der Installation bereits die Prüfung geben, zum anderen verändert sich Windows 10 bei jedem Update.

Lösung: Die Antwort b. ist richtig. Bei Windows 10 handelt es sich um ein Cloud-unterstütztes Betriebssystem. Wer Windows 10 einführt, führt auch Cloud-Dienste im Unternehmen ein. Allein dieser Umstand zeigt, dass eine Datenschutz-Folgenabschätzung nach DSGVO stattfinden sollte, bevor Windows 10 zum Einsatz kommt. Zudem haben die Aufsichtsbehörden für den Datenschutz klar gemacht: Jedes Update bei Windows 10 führt dazu, dass ein neues Produkt vorliegt, dessen Einsatz erneut auf die datenschutzrechtliche Zulässigkeit geprüft werden muss.