Newsletter Datenschutz

Ausgabe 02 | 2023

Auftragsverarbeitung im Fokus der Datenschutz-Aufsicht

Ihr Datenschutz-Info Blatt

Liebe Leserin, lieber Leser,
warum nur dieser Aufwand? Das fragen sich viele, wenn es um den Datenschutz geht. Es ist deshalb wichtig, zu verstehen, warum die Datenschutz-Maßnahmen notwendig sind. So erfahren Sie zum Beispiel in dieser Ausgabe, weshalb Sie noch mehr für die Sicherheit Ihres Smartphones und für den Datenschutz bei Filesharing tun sollten.

Andererseits glauben viele, inzwischen wären alle Fragen zu Datenübermittlungen in die USA geklärt, weiterer Aufwand zur Prüfung sei nicht mehr erforderlich. Das stimmt aber so nicht. Lesen Sie, was bisher wirklich in Richtung Datenschutzabkommen mit den USA passiert ist.

Aber auch die Aufsichtsbehörden unternehmen gegenwärtig besondere Anstrengungen, zum Beispiel bei Prüfungen zur Auftragsverarbeitung. Lernen Sie die Hintergründe kennen, die zeigen, warum die Aufwände für den Datenschutz gerechtfertigt sind.

Ich wünsche Ihnen viel Spaß beim Lesen!

Ihr Frank Berns, Datenschutzbeauftragter

Ist Ihr Smartphone sicher genug?

Smartphones sind für viele zum täglichen Begleiter geworden. Trotzdem wird die Sicherheit bei Smartphones weiterhin vernachlässigt. Das kann gefährliche Folgen haben. Denn Smartphones dienen zunehmend als Identitätsnachweis.

Ohne Smartphone geht es für viele nicht mehr

„Die Faszination für Smartphones ist so groß wie nie“, so Markus Haas, Präsidiumsmitglied im Digitalverband Bitkom. „Sie informieren und unterhalten uns, steigern unsere Produktivität und unterstützen uns in vielen Lebenslagen. Smartphones stehen für Innovation und Wachstum.“

Dies bestätigt eine Bitkom-Umfrage: Für nahezu alle Nutzerinnen und Nutzer (96 Prozent) sind Smartphones eine große Erleichterung im Alltag. Neun von zehn (90 Prozent) können sich ein Leben ohne Smartphone nicht mehr vorstellen.
Umso wichtiger ist es, für die notwendige Datensicherheit bei den Smartphones zu sorgen.

KONTAKT zu uns MAIL@Konzept17.de

Smartphones werden immer noch schlechter als PCs geschützt

Obwohl es gerade die smarten Funktionen zusätzlich zum Telefonieren sind, die die Smartphones so beliebt machen, denken immer noch viele Nutzerinnen und Nutzer, sie hätten ein „Handy" dabei, also ein Mobiltelefon. Doch bekanntlich sind Smartphones mehr Computer als Telefon.

Trotzdem werden Computer wie PCs und Notebooks anders und besser abgesichert als Smartphones, wie aktuelle Umfragen belegen.

Mit 96 Prozent haben fast alle Smartphone-Nutzer eine Bildschirmsperre eingestellt, neun von zehn (90 Prozent) haben einen SIM-Karten-Schutz aktiv. Dabei sperrt sich das Handy, sobald die SIM-Karte entfernt wird. Aber nur etwa jeder Zweite (55 Prozent) erstellt auch regelmäßig Backups seiner Smartphone-Daten. Virenschutzprogramme haben 43 Prozent installiert. Jeder Sechste (16 Prozent) deckt seine Smartphone-Kamera ab.

Wie ist es bei Ihnen? Schützen auch Sie Ihren „täglichen Begleiter" Smartphone schlechter als den PC?

Bedeutung des Smartphones steigt und damit die Risiken

Bereits 13 Prozent nutzen einen Passwort-Safe, um Passwörter auf dem Smartphone zentral zu verwalten. Das ist nur ein Beispiel dafür, dass Smartphones zunehmend als Sicherheitswerkzeuge genutzt werden. Smartphones sind auch die häufigste Basis für den zweiten Faktor bei Online-Banking und Online-Shopping, zum Beispiel über den Fingerabdruck-Sensor.

Denkt man dann noch an mobiles Bezahlen per Smartphone, an digitale Impfzertifikate und Pläne für digitale Ausweise, die auf dem Smartphone gespeichert werden, ist schnell klar, dass Smartphones zu einem immer größeren Sicherheitsrisiko werden, wenn der Smartphone-Schutz nicht stimmt.

Denken Sie an die Smartphone-Sicherheit, im Privatleben und im Beruf

Gleich ob Sie Ihr Smartphone nur privat oder auch beruflich nutzen: Überprüfen Sie umgehend, ob Sie diesen Schutz bereits aktiv haben:

- regelmäßig Smartphone-Betriebssysteme wie Android oder iOS aktualisieren
- regelmäßig Updates für Apps installieren
- Bildschirmsperre nutzen
- in aller Regel bereits verfügbare Verschlüsselung für die Daten auf dem Smartphone nutzen
- keine Apps außerhalb der App-Stores installieren
- Verbindungen über WLAN und Bluetooth nach Nutzung abschalten
- an Diebstahl- und Verlustrisiko denken
- eine professionelle Sicherheits-App installieren

Schützen Sie Ihren „täglichen Begleiter", um die Vorteile eines Smartphones ohne die damit verbundenen Datenrisiken nutzen zu können!

Der Weg zum Privacy Shield II

Datenübermittlungen in die USA sind für viele Unternehmen wichtiger denn je. Tragfähige Rechtsgrundlagen hierfür fehlen jedoch zum Teil. Gerade Praktiker warten deshalb dringend auf den „Privacy Shield II". Lesen Sie, was es damit auf sich hat und wann dieser „Schild" verfügbar sein könnte.

Angemessenheitsbeschluss heißt das Zauberwort

Die USA sind in der Sprache der Datenschutz-Grundverordnung (DSGVO) ein Drittland, also ein Land außerhalb des Geltungsbereichs der DSGVO. Datenübermittlungen dorthin sind zulässig, wenn die Europäische Kommission beschlossen hat, dass dort ein angemessenes Schutzniveau herrscht. Sobald ein solcher Beschluss vorliegt, bedürfen Datenübermittlungen keiner besonderen Genehmigung durch die Aufsichtsbehörden. So regelt es Art. 45 Abs. 1 DSGVO.

Mit dem Privacy Shield I war etwa vier Jahre lang alles gut

Eine solchen Beschluss der Europäischen Kommission gab es tatsächlich schon einmal. Er betraf den „Privacy Shield I". Dabei handelte es sich um Datenschutzvorkehrungen, die zwischen der EU und den USA für Datenübermittlungen in die USA vereinbart worden waren. Mitte Juli 2016 fasste die Europäische Kommission auf ihrer Basis einen Angemessenheitsbeschluss. Er hielt fast auf den Tag genau vier Jahre. Am 16. Juli 2020 erklärte der Europäische Gerichtshof (EuGH) den Beschluss allerdings für nichtig. Das geschah durch das Urteil „Schrems II".

Seit 2020 bemüht man sich um einen Privacy Shield II

Seither herrscht eine gewisse rechtliche Konfusion. Natürlich gibt es durchaus noch einige andere Rechtsgrundlagen für Datenübermittlungen in die USA, etwa eine Einwilligung des Betroffenen. Sie verursachen aber viel Aufwand und sind für eine Übermittlung von Daten vieler Personen praktisch fast nicht zu handhaben. Deshalb haben die USA und die EU nach der Entscheidung „Schrems II" sofort damit begonnen, den für nichtig erklärten „Privacy Shield I" durch einen „Privacy Shield II" zu ersetzen. Diese Bemühungen sind jetzt in ein entscheidendes Stadium getreten.

Dem EuGH missfielen am Privacy Shield I zwei zentrale Punkte

Den EuGH störten am „Privacy Shield I" vor allem zwei Dinge:

- Zum einen monierte er, dass die US-Geheimdienste nach dem Recht der USA in keiner Weise an den Grundsatz der Verhältnismäßigkeit gebunden sind, wenn sie personenbezogene Daten erheben.
- Zum anderen rügte er, dass Nicht-US-Bürger gemäß dem Recht der USA keinerlei Rechtsschutz gegen derartige Datenerhebungen hätten.

US-Präsident Biden hat mit einer Executive Order reagiert

Die USA haben sich vom Prinzip her bereit erklärt, diese beiden Schwachstellen zu beheben. Das ist nach dem Recht der USA allerdings gar nicht so einfach. Beschritten wurde der Weg, dass US-Präsident Biden am 07.10.2022 eine sogenannte „Executive Order" erlassen hat. Dabei handelt es sich um eine

verbindliche Anweisung des Präsidenten an alle US-Bundesbehörden. Damit gilt sie auch für alle US-Geheimdienste. Denn Geheimdienste gibt es in den USA nur auf Bundesebene.

Die Executive Order legt den Geheimdiensten gewisse Fesseln an

Bisher konnten die US-Geheimdienste selbst entscheiden, welche Maßnahmen zur Beschaffung und Auswertung von Daten sie für erforderlich hielten. Künftig müssen sie jedes Jahr im Voraus eine Art Rahmenplan erstellen. Er bedarf der Billigung durch den jeweiligen US-Präsidenten. Veröffentlicht wird er jedoch selbstverständlich nicht. Zugleich hat die Executive Order eine Institution eingerichtet, die sie als „Data Protection Review Court" bezeichnet. Dieses „Gericht" soll auch Nicht-US-Bürgern Rechtsschutz gewähren.

Jetzt ist die Europäische Kommission am Zug

Nun liegt der Ball, bildlich gesprochen, bei der Europäischen Kommission. Sie muss sich darüber einig werden, ob die getroffenen Maßnahmen der USA ausreichen, um einen Angemessenheitsbeschluss erlassen zu können. Erst wenn das geschehen ist, hat die Praxis wieder eine Rechtsgrundlage, die in ihrer Wirkung dem früheren Privacy Shield I entspricht. Die Diskussion darüber, ob ein solcher Angemessenheitsbeschluss möglich ist, läuft im Augenblick. Einbezogen sind dabei intern auch die Aufsichtsbehörden der EU-Mitgliedstaaten. Belastbare Ergebnisse sind noch nicht bekannt.

Möglicherweise gibt es im April 2023 den Durchbruch

Selbstverständlich gibt es Stimmen, die den jetzt gewählten Lösungsansatz kritisieren. Mit an der Spitze steht dabei Herr Schrems, Rechtsanwalt in Österreich, nach dem gleich zwei EuGH-Urteile benannt sind. In Brüssel ist zu hören, dass man sich bis etwa April 2023 einen Angemessenheitsbeschluss zutraut. Die Praktiker in den Unternehmen wären mit Sicherheit begeistert, wenn dies gelingen würde.

Auftragsverarbeitung im Fokus der Datenschutz-Aufsicht

Kommen externe Dienstleister ins Spiel, kann eine Auftragsverarbeitung vorliegen. Lesen Sie, warum dieses Thema gerade jetzt besonders aktuell ist.

Ausgangspunkt sind Webhosting-Verträge

Ohne Internetseite kommt heute kein Unternehmen mehr aus. Zahlreiche Unternehmen haben außerdem einen Online-Shop. Gerade während Corona haben sich Online-Shops vielfach als unentbehrlich erwiesen. Um Webseiten und Online-Shops professionell betreiben zu können, wird in aller Regel ein externer Dienstleister eingeschaltet, also ein Webhoster. Er arbeitet auf der Basis eines Webhosting-Vertrags.

Webhosting ist Auftragsverarbeitung

Dass Webhosting eine Auftragsverarbeitung im Sinn der DSGVO darstellt, ist allgemeine Meinung. Denn der Auftraggeber macht dem Webdesigner genaue Vorgaben dafür, wie seine Internetseite und/oder

sein Online-Shop betrieben werden sollen. In der Sprache des Datenschutzrechts handelt es sich dabei um Weisungen des Auftraggebers an den Auftragsverarbeiter.

Die Aufsichtsbehörden sind vielfach unzufrieden

Die Datenschutz-Aufsichtsbehörden haben prinzipiell nichts gegen Auftragsverarbeitung. Allerdings rügen sie häufig, dass aus ihrer Sicht in den Verträgen über die Auftragsverarbeitung wichtige Details fehlen. Außerdem beanstanden sie immer wieder, dass zwar von der Papierform her alles korrekt wirkt, es aber an einer ausreichenden praktischen Umsetzung der vertraglichen Regelungen fehlt.

Sie führen deshalb eine gemeinsame Prüfaktion durch

Ob die Kritik der Aufsichtsbehörden immer wirklich berechtigt ist, kann dahinstehen. Viel entscheidender ist, dass gleich sechs Aufsichtsbehörden vereinbart haben, das Thema „Auftragsverarbeitung beim Webhosting“ gemeinsam aufzugreifen. Dabei handelt es sich um die Aufsichtsbehörden von Bayern, Berlin, Niedersachsen, Rheinland-Pfalz, Sachsen und Sachsen-Anhalt. Seit Mitte 2022 führen sie eine sogenannte koordinierte Prüfung durch. Dies bedeutet, dass sie eine gemeinsame Checkliste entwickelt haben. Auf ihrer Basis treten sie an Unternehmen heran und stellen eingehende Fragen.

Unternehmen dürfen Anfragen nicht ignorieren

Die beteiligten Aufsichtsbehörden schreiben eine große Zahl von Unternehmen an und fordern sie auf, zunächst einen umfassenden Fragebogen auszufüllen. Dies löst beträchtlichen Aufwand aus. Viele Fragen lassen sich nicht sorgfältig beantworten, ohne vorher die Abläufe im Unternehmen umfassend durchzugehen. Dies berührt dann oft auch Abteilungen, die beispielsweise mit dem Online-Shop an sich unmittelbar nichts zu tun haben. Es geht aber nicht anders. Denn ein Unternehmen, das Fragen unvollständig oder sogar falsch beantwortet, riskiert eine Geldbuße.

Die Prüfaktion hat so etwas wie Fernwirkungen

Jedem Fachmann ist klar: Falls die Prüfaktion zum Webhosting aus der Sicht der Aufsichtsbehörden relevante Erkenntnisse bringt, werden ähnliche Prüfaktionen folgen. Dabei wird es jeweils um unterschiedliche Formen der Auftragsverarbeitung gehen. Das ist der Grund dafür, warum das Thema Auftragsverarbeitung insgesamt momentan einige Wellen schlägt.

Ohne Vertrag ist Auftragsverarbeitung nicht erlaubt

Gar nicht selten kommt es vor, dass eine Auftragsverarbeitung vorliegt und auch ein zuverlässiger Auftragsverarbeiter als Dienstleister tätig ist. Einen schriftlichen Vertrag gibt es allerdings nicht. Man meint vielmehr, entsprechende Auftragsscheine und Abrechnungen würden ausreichen. Das sieht die DSGVO allerdings anders:

1. Sie legt fest, dass ein ausdrücklicher Vertrag nötig ist.
2. Sie macht genaue Vorgaben zu seinem Inhalt.
3. Sie fordert einen dokumentierten Vertragstext (schriftlich oder elektronisch).

Das Thema „Unterauftrag“ verlangt besondere Aufmerksamkeit

Beim Thema „Unterauftrag“ ist die DSGVO ebenso klar und eindeutig. Sie legt fest, dass ein Auftragsverarbeiter nur dann einen weiteren Auftragsverarbeiter einschalten darf, wenn der

Auftraggeber dies schriftlich genehmigt hat. Hier geht es also nicht ohne Schriftform. Manchmal liegt ein Vertrag vor, der Unteraufträge nicht vorsieht. Dann entsteht aber trotzdem kurzfristig der Bedarf, einen Unterauftragnehmer einzuschalten. Der Vertrag muss deshalb nicht unbedingt geändert werden. Nötig ist dann aber jedenfalls eine schriftliche Erlaubnis.

Bitte bleiben Sie geduldig

Nachfragen zum Thema Auftragsverarbeitung können durchaus nerven, vor allem wenn gerade viel los ist. Angesichts der Aktionen der Aufsichtsbehörden haben sie allerdings gute Gründe. Deshalb kooperieren Sie bitte.

So wird Filesharing nicht zum Risikoaustausch

In Zeiten von Homeoffice und mobiler Arbeit müssen auch größere Dateien mit anderen Nutzenden ausgetauscht werden. Datenaustausch über Filesharing-Dienste ist deshalb beliebt, leider aber nicht automatisch sicher. Denken Sie an zusätzliche Schutzmaßnahmen.

Das Problem der großen Dateien

Von zu Hause aus zu arbeiten, ist seit Ausbruch der Corona-Pandemie zur neuen Normalität in der Arbeitswelt geworden. Auch in Zukunft werden dezentrale und hybride Arbeitsformen weiter an Bedeutung gewinnen, versichern Marktforscher. Doch was bedeutet das für Ihren Arbeitsalltag?

Ob Sie selbst im Büro, im Homeoffice oder unterwegs sind – es ist nur eine Frage der Zeit, dass Sie eine große Datei verschicken müssen. Sei es die neue Kundenpräsentation, das hochauflösende Foto vom neuen Messestand oder die Demo-Version einer Software, die ein Kollege beim Kunden vorstellen soll.

Wie aber überträgt man große Dateien? Als E-Mail-Anhang? Nicht nur die oftmals fehlende E-Mail-Verschlüsselung kann hier ein Problem sein. Große Dateien sind nicht wirklich als E-Mail-Anhang geeignet, entsprechend warnen viele E-Mail-Programme bereits beim Versuch.

Filesharing ist zunehmend beliebt

Anstatt die großen Dateien direkt per E-Mail zu verschicken, reicht es bei Filesharing-Diensten, einen Link als E-Mail zu versenden. Zuvor lädt man die Dateien in ein Filesharing-Verzeichnis und erzeugt den Link, den der Empfänger erhalten soll.

Das klingt einfach. Ist es auch, aber leider ist es nicht automatisch sicher, die Dateien über einen Filesharing-Dienst auszutauschen.
Das beginnt bereits damit, dass Sie sich fragen sollten, wohin Sie eigentlich die Dateien übertragen, damit sie in dem Austauschverzeichnis liegen. Meist steckt ein Cloud-Dienst dahinter, oftmals betrieben von einem Anbieter jenseits der Europäischen Union. So stellt sich bei personenbezogenen Daten die Frage, ob die Übertragung an den Filesharing-Dienst denn zulässig ist oder nicht.

Unklarer Speicherort, unsicherer Versand von Links

Neben der Frage, wohin Sie eigentlich die Dateien, die Sie austauschen möchten, übertragen, sollten Sie bei Filesharing auf die Datensicherheit achten. Erscheint der Datenaustausch sehr komfortabel, ist er leider meist nicht sicher genug. Generiert der Dienst zum Beispiel einen Link, den Sie auf Knopfdruck an eine E-Mail-Adresse Ihrer Wahl versenden können, erzeugt das eine einfache E-Mail, die jeder Empfänger öffnen und bei der jeder auf den Link klicken kann. Ein Fehler in der E-Mail-Adresse führt dann dazu, dass womöglich unbefugte Dritte die Datei herunterladen können.

Besser ist es, wenn der Link allein nicht ausreicht, sondern ein Einmal-Passwort erzeugt wird, das der Empfänger benötigt und das auf einen anderen Weg an den Empfänger übertragen wird. Ein Passwort, das in der gleichen E-Mail steht wie der Link ist, bringt dagegen nichts.

Prüfen Sie also genau, welche Sicherheitsfunktionen der Filesharing-Dienst, den Sie nutzen möchten, anbietet. Verwenden Sie beruflich nur den Filesharing-Dienst, der im Unternehmen zugelassen ist.

Denken Sie auch an die Risiken, wenn Sie selbst einen Link erhalten, um über Filesharing eine größere Datei herunterladen zu können. Ist es wirklich der angegebene Absender? Was verbirgt sich tatsächlich hinter dem Link? Ist die Datei womöglich verseucht?

Sie sehen: Filesharing-Dienste vereinfachen zwar den Datenaustausch. Sie liefern aber nicht automatisch Sicherheit mit. Daher können mit dem Datenaustausch leicht zu übersehende Risiken verbunden sein.

Wissen Sie, was zu sicherem Filesharing gehört? Machen Sie den Test!

Frage: Dateien aus Filesharing-Diensten sind immer virenfrei. Stimmt das?

1. Nein. Gelangt Malware in das Austauschverzeichnis, könnte sich die Malware auch hinter dem generierten Link verbergen, der per E-Mail verteilt wird.
2. Ja, Filesharing ist immer mit einem Malware-Schutz verknüpft, der melden würde, wenn es sich um Schadsoftware handelt.

Lösung: Die Antwort 1. ist richtig. Sie können nicht davon ausgehen, dass die Dateien, die in einem Austauschverzeichnis liegen, auf Malware hin untersucht wurden. Prüfen Sie also selbst, ob die Dateien verseucht sind, bevor Sie diese übertragen. Als Empfänger eines Links sollten Sie diesen mit einem Link-Scanner überprüfen, bevor Sie die Datei herunterladen.

Frage: Die Datei, zu der der Link führt, liegt auf dem Computer des Absenders. Ist das so?

1. Ja, der Filesharing-Dienst stellt nur die Verbindung zwischen den Rechnern her.
2. Nein, die Datei wird zuvor auf der Filesharing-Plattform abgelegt, also dort zwischengespeichert.

Lösung: Die Antwort 2. ist richtig. Bei Filesharing geht es nicht um die Verknüpfung von Computern, sondern um die Übertragung von Dateien. Anstatt eine Datei direkt zu verschicken, lädt man sie bei Filesharing auf eine Plattform. Von dort lädt sie der Empfänger dann herunter. Deshalb wird die Datei an einen Dritten, den Filesharing-Betreiber, übertragen und von ihm gespeichert. Entsprechend muss bei dem Betreiber geklärt sein, ob der Datenschutz angemessen ist.

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