5/2021
97 – 120

Kurzmeldung
Anonymisierung Rsp
Viktoria Haidinger

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Internationaler Datenverkehr – welcome back

Neue Standardvertragsklauseln/Standarddatenschutzklauseln

Rainer Knyrim und Marek Gerhalter

Der Schlüssel zur Cloud liegt beim Kunden

Interview mit Andreas Wurm, Datenschutzkoordinator Emakina

OGH: (Inter-)nationale Zuständigkeit für datenschutzrechtliche Ansprüche

Christian Wirthensohn

Digitale Interaktion mit (Potenzial-)Kunden (Teil 2)

Gerhard Kunnert

Checkliste: Privacy by Design/Default bei Software (Teil 2)

Hans-Jürgen Pollirer

OGH: Speicherdauer von Bonitätsdaten

Viktoria Haidinger und Michael Löffler

FAQ: Darf ich die 3-G-Nachweise meiner Mitarbeiter kontrollieren?

Viktoria Haidinger

ISSN 2313-5409

dako.manz.at

MANZ

Österreichische Post AG PZ 18Z041356 P Verlag Manz, Gutheil Schoder Gasse 17, 1230 Wien

Rainer Knyrim/Reinhard Ebner
Rechtsanwalt und Partner bei Knyrim Trieb Rechtsanwälte/freier Journalist

Der Schlüssel zur Cloud liegt beim Kunden

Interview mit Andreas Wurm, Datenschutzkoordinator Emakina. Die Nutzung von Cloud-Diensten ist heute gang und gäbe. Bei der Verarbeitung personenbezogener Daten sind hier besondere Vorkehrungen zu treffen. Was aber, wenn der Cloud-Anbieter einem US-Konzern gehört? Die Abwicklung eines derartigen Projekts erläutert Andreas Wurm.

Datenschutz konkret: Sie sind für den Digital Business-Dienstleister Emakina tätig und haben als Auftragsverarbeiter ein komplexes Projekt umgesetzt. Können Sie kurz die Ausgangslage schildern?
Andreas Wurm: Es handelte sich um ein CRM-Projekt, bei dem sensible Daten in der Cloud verarbeitet werden. Komplex wurde die Ausgangssituation aufgrund der Tatsache, dass der verwendete Cloud-Anbieter einen US-amerikanischen Mutterkonzern hat.

Für eine rechtskonforme Lösung sollten die Daten daher grundsätzlich in Europa gespeichert werden. Dafür nutzen wir zwei europäische Datenzentren, die in Deutschland und Frankreich angesiedelt sind. Diese interne Redundanz sorgt für zusätzliche Ausfallssicherheit.

Ein wesentlicher Faktor, um derartige Projekte auf den Boden zu bringen, ist eine gute Zusammenarbeit aller Beteiligter. Nur so ist es möglich, alle für die anstehenden Entscheidungen notwendigen Informationen zu sammeln und sich über Aufgabenverteilung und erforderliche Spezifikationen klar zu werden. In diesem Fall war der Wille zur Zusammenarbeit von Anfang an da; so konnten wir zu einem tragfähigen Rahmen für die Verarbeitung der personenbezogenen Daten finden, der die Anforderungen des Kunden, der DSGVO und der Sicherheit gleichermaßen erfüllt.

Datenschutz konkret: Der Kunde wollte bei der Gelegenheit auch gleich auf ein neueres System wechseln. Warum?
Wurm: Oftmals braucht es diesen Systemwechsel, um sozusagen aus den alten Silos herauszukommen. Veraltete Systeme sind schwerer zu warten. Durch eine Erneuerung lässt sich den Sicherheitsanforderungen Genüge tun und den modernen Standards entsprechen.

Es ist immer schwierig, ältere Systeme auf dem aktuellen Stand der Technik zu halten, gerade weil neuere Technologien häufig vom Hersteller nicht unterstützt werden. Gelegentlich fehlt es auch am Personal mit dem nötigen Wissen, um diese in die Jahre gekommenen Systeme zu administrieren. Irgendwann kommt daher der Punkt, an dem eine Erneuerung unausweichlich wird.

Beim besprochenen Projekt war der Systemwechsel auch der Innovationskraft des Unternehmens selbst geschuldet, das sich dadurch einen Wettbewerbsvorteil sichern wollte. Mit der Digitalisierung der Geschäftsprozesse wurden gleich mehrere Ziele verfolgt: Den Kunden sollten mehr Services geboten werden sowie moderne Interfaces, um über digitale Kanäle mit dem Unternehmen in Verbindung zu treten oder zu bleiben. Die eigenen Mitarbeiter wiederum sollten ihre täglichen Aufgaben durch modernere Tools besser erfüllen können.

Datenschutz konkret: Eine Besonderheit in diesem Fall: Der Cloud-Anbieter gehört einem US-Konzern. Aufgrund der *Schrems II*-Entscheidung des EuGH ist das eine problematische Konstellation. Wie ist man mit diesem Problem umgegangen?
Wurm: Die Frage war, wie eine rechtskonforme Verarbeitung ermöglicht werden könnte. Wir haben daher die verschiedenen Anforderungen und Branchenerfordernisse analysiert und im Anschluss ein entsprechend enges Netz an technischen und organisatorischen Maßnahmen gezogen, um diese Rechtskonformität gewährleisten zu können. Wir haben uns mit dem Kunden und seinen Rechtsberatern zusammengesetzt und unsere Standpunkte diskutiert.

Datenschutz konkret: Die Idee war, die Cloud in Europa zu hosten und auf den Support des ursprünglichen Cloud-Anbieters nicht zurückzugreifen. Wie wurde das umgesetzt?
Wurm: Für Supportfälle haben wir einen Rahmen geschaffen, bei dem der Datenzugriff gar nicht mehr beim Cloud-Anbieter selbst erfolgt. In der Auftragsverarbeitervereinbarung wurde festgehalten, dass Emakina den Support inhouse durchführt und dass kein Zugriff ohne Zustimmung des Verantwortlichen erfolgen kann.

Der Schlüssel zur Verarbeitung personenbezogener Daten auf der Cloud-Plattform wird vom Kunden selbst verwahrt.

Datenschutz konkret: Theoretisch könnten die US-Behörden auf Basis des Cloud Acts den Zugriff auf Daten in den deutschen und französischen Rechenzentren einfordern. Wie wurden dagegen auf technischer Seite Vorkehrungen getroffen?
Wurm: Wir haben das über modernste Verschlüsselungstechnologie gelöst. Auf eine einfache Ebene heruntergebrochen: Wir haben einen Schlüssel, der Daten unkenntlich macht. Er wird auch gebraucht, um sie wieder lesbar zu machen.

Der Schlüssel wiederum wird von sog Secrets geschützt; diese bestehen aus zwei Teilen: Der eine Teil wird von der Plattform in Form eines Master Secrets in jeder Produktiteration neu zu Verfügung gestellt, der andere Teil ist kundenspezifisch. Für die Generierung von Letzterem gibt es verschiedene Möglichkeiten. Der Kunde hat sich für jene Option entschieden, bei der er diesen Teil selbst beibringt, und zwar nicht nur einmal, sondern zu jeder Zeit im Zuge der Datenverarbeitung. Dh, der Schlüssel ist im System des Kunden verwahrt und wird nur bei Bedarf von der Plattform abgerufen.

Datenschutz konkret: Mit anderen Worten: Der Kunde kann den Schlüssel jederzeit unbrauchbar machen und die Daten so vor unbefugtem oder unerwünschtem Zugriff schützen?
Wurm: Die Kontrolle liegt jederzeit beim Kunden. Es handelt sich um eine sog „Bring Your Own Key"-Lösung; also um ein Kon-

zept der nutzerdefinierten Verschlüsselung von Cloud-Diensten, bei der nicht der Cloud-Anbieter, sondern der Anwender bzw Kunde selbst seinen Schlüssel verwaltet.

Es gibt verschiedene Möglichkeiten, das in der Praxis zu implementieren. Wir haben uns für eine Lösung entschieden, bei der der Schlüssel in einem Zwischenspeicher verwahrt und bei jeder Verarbeitung neu zur Verfügung gestellt wird. Er kann jederzeit invalidiert werden, eine weitere Datenverarbeitung würde damit unterbunden.

Andreas Wurm
© Foto Mario Wohlschlager

Datenschutz konkret: Auf vertraglicher Seite wurden vom Kunden die neuen Art 28 DSGVO-Standardvertragsklauseln als Vertragsbasis herangezogen. Für den Fall eines versuchten Zugriffs aus den USA wurden zusätzlich Klauseln eingebaut, wie sie seitens des EDSA für den internationalen Datentransfer empfohlen werden. Wie war es für Sie, mit diesen vertraglichen Aspekten umzugehen?

Wurm: Das machte natürlich einiges an Abstimmungsbedarf auf unserer Seite notwendig. Je klarer die Kundenanforderungen sind, desto einfacher wird das aber. In diesem Fall haben glücklicherweise alle Beteiligten an einem Strang gezogen.

Datenschutz konkret: Als Auftragsverarbeiter übernehmen Sie Haftung für das, was Sie ausliefern?

Wurm: Es brauchte ein Konstrukt, bei dem alle Beteiligten einen Teil der Haftung übernehmen. Wir haben eine tragfähige Lösung gefunden, mit der eine langfristige vertrauensvolle Zusammenarbeit sichergestellt ist.

Datenschutz konkret: Mit welchem Zeitrahmen muss man für die Umsetzung eines derartigen Projekts rechnen? Wie hoch ist der technische Aufwand für die Datenschutzkomponente?

Wurm: Ich muss hier leider eine typische Beraterantwort geben: Es kommt darauf an. Es kommt auf das Commitment von allen Seiten an, auf das Buy-in vom Management und von den technischen Playern auf Kundenseite, denn nur dann lässt sich eine effiziente Umstellung bewerkstelligen.

Ein weiterer Faktor ist die Komplexität der zu Grunde liegenden Verarbeitungsaktivität. Es macht einen Unterschied, ob ich einen Newsletter implementiere oder zB eine Datenbank im politischen Bereich erstelle. Je mehr Expertise im Projektteam vorhanden ist, umso effizienter gelingt die Abwicklung. Und es lohnt sich auch, vorab in eine ausgiebige Analyse zu investieren.

Datenschutz konkret: Für Sie war es das erste Projekt nach dem neuen Regelwerk. Welche Lektionen und Erfahrungen können Sie davon ausgehend an andere Auftragsverarbeiter weitergeben?

Wurm: Unabdingbar ist es, das Datenschutzthema von Anfang eines Projekts an einzuplanen. Das ist heute einfach nicht mehr wegzudenken. Als überzeugter Europäer freue ich mich darüber, dass das Bewusstsein für diese Thematik mittlerweile ein hohes ist.

Zunächst gilt es, die Frage nach den Kerngeschäftsprozessen zu stellen und danach zu definieren, was diese mit der Verarbeitung personenbezogener Daten zu tun haben. So früh wie möglich ist dann in einen iterativen Prozess zu gehen, um sich der Lösung oder dem Ziel anzunähern. Anstatt ein riesiges Ausschreibungsverfahren zu starten, ist es oftmals sinnvoller, das Projekt in kleineren Schritten, aber umso nachhaltiger abzuwickeln.

Hilfreich ist es auch, sich – wo nötig – von außen Expertise zu holen. Was möchte ich erreichen und was brauche ich dafür? Ich rate immer davon ab, nur um der Digitalisierung willen zu digitalisieren. Datenschutz ist jedoch ein wichtiges Thema, weil er ein unverzichtbares Element für die erfolgreiche Zukunft eines Unternehmens ist.

Dako 2021/56

Zum Thema

Über den Interviewpartner

Mag. Andreas Wurm studierte Betriebswirtschaft mit Schwerpunkt Informationswirtschaft an der WU Wien und absolvierte eine Ausbildung zum geprüften Datenschutzbeauftragten. Im IT-Bereich ist Wurm seit 2009 beruflich tätig. 2016 begann er seine Arbeit für die Emakina Central & Eastern Europe GmbH. Seit 2019 ist er als Operational Excellence Lead Teil des Managementteams des auf Digital Business spezialisierten IT-Dienstleisters. In seiner Funktion zeichnet Andreas Wurm für die Bereiche Agile Advisory, Quality Assistance, IT-Operations und Compliance verantwortlich. Darüber hinaus agiert er als Datenschutzkoordinator für die Wiener Niederlassung der Emakina-Gruppe. E-Mail: a.wurm@emakina.at

Factbox Emakina Central & Eastern Europe GmbH

Emakina CEE ist Teil der 2001 gegründeten börsennotierten Brüsseler Emakina Group mit über 1.000 Beschäftigten in 20 Ländern. Der Umsatz betrug 2020 99 Mio Euro. Aufgabe von Emakina ist, die Kundenbeziehungen von Unternehmen mit unterschiedlichen digitalen Tools zu stärken. Dazu zählen CRM-Projekte, Omnichannel-Commerce, die Entwicklung und Gestaltung von Websites und CMS, Automatisierungslösungen für digitales Marketing sowie Advanced-Analytics-Projekte.
Zu den Kunden zählen ua Asfinag, Austrian Standards, Billa, FC Red Bull Salzburg, Hartlauer, Kastner & Öhler|Gigasport, Julius Meinl, Konica Minolta, POC Sports und der Tourismusverband Wien.