SANOVIS CONSULTING WITH CARE.

CURACON SICHERHEIT GEBEN. LÖSUNGEN BIETEN.

NEWSLETTER DATENSCHUTZ

Liebe Leserin, lieber Leser,

wieder einmal hat ein Urteil des Europäischen Gerichtshofs (EuGH) die Datenschutz-Welt durcheinandergewirbelt. Betroffen sind insbesondere die Nutzer von Online-Diensten, die in den USA betrieben werden, und damit sehr viele Unternehmen in Deutschland.
Die ersten beiden Artikel dieser Ausgabe informieren Sie deshalb über die rechtlichen Hintergründe, aber auch über aktuelle Angebote im Bereich Verschlüsselung, die mehr versprechen, als sie halten können.
Ein Dauerbrenner im Datenschutz ist die Videoüberwachung, die häufig auch auf Baustellen stattfindet. Erfahren Sie, was hierbei aus Datenschutzsicht zu beachten ist. Der vierte Beitrag geht auf das Problem ein, dass manche Maßnahmen im Datenschutz nicht wirksam sind. Lesen Sie, wie sich das verhindern lässt und welche Rolle Ihnen dabei zukommt.
Wir wünschen Ihnen interessante Erkenntnisse beim Lesen!

Dr. Uwe Günther
Beratungsfeldleiter Datenschutz, Curacon GmbH
Geschäftsführer, Sanovis GmbH

Stefan Strüwe
Beratungsfeldleiter Datenschutz, Curacon GmbH

Oktober_2020

1 DATENÜBERMITTLUNG IN DIE USA – AUCH OHNE PRIVACY SHIELD?

Nahezu jedes Unternehmen übermittelt Daten in die USA. Seit Kurzem hört man viel vom „Ende des Privacy Shield“. Auf den ersten Blick scheint das ein Thema nur für Spezialisten. Es hat aber Auswirkungen auf den Alltag im Unternehmen.

Übermittlungen in die USA nur bei angemessenem Datenschutzniveau

Die USA sind kein Teil der Europäischen Union, sie sind vielmehr ein „Drittstaat“. Die Übermittlung von personenbezogenen Daten in die USA ist deshalb an besondere Voraussetzungen gebunden. Sie ist nur zulässig, soweit in den USA ein „angemessenes Datenschutzniveau“ herrscht.

Der Privacy Shield – bisher praktisch und bequem

An dieser Stelle kommt der „Privacy Shield“ ins Spiel. Es handelte sich dabei um eine Art Register. Jedes US-Unternehmen, das bestimmte Voraussetzungen des Datenschutzes erfüllte, konnte sich dort eintragen lassen. Die Europäische Kommission hatte förmlich festgelegt: Wenn ein US-Unternehmen registriert ist, herrscht in diesem Unternehmen ein angemessenes Datenschutzniveau. Über 5.500 US-Unternehmen haben diese Möglichkeit genutzt. Dazu gehören auch Internet-Giganten wie Google.

Europäische Unternehmen als Nutznießer

Nutznießer dieses Verfahrens waren vor allem die europäischen Geschäftspartner der registrierten US-Unternehmen. Diese Geschäftspartner konnten an ihre US-Partner personenbezogene Daten genauso leicht übermitteln wie an Geschäftspartner innerhalb der Europäischen Union. Das war praktisch und bequem.

Der Privacy Shield – aus und vorbei!

Mitte Juli 2020 stoppte der Europäische Gerichtshof diese Verfahrensweise. Er stellte fest, dass der „Privacy Shield“ gerade nicht für ein angemessenes Datenschutzniveau bei den registrierten US-Unternehmen sorgt. Die Folge: Vielen Datenübermittlungen in die USA fehlt jetzt eine tragfähige rechtliche Grundlage.

Schwierige Situation für alle Unternehmen

Das Urteil wirkte wie ein Keulenschlag. Es räumt keinerlei Übergangsfrist ein. Die Rechtsgrundlage „Privacy Shield“ fiel über Nacht weg. Das führt im Augenblick zu folgender Situation:

- In manchen Fällen gibt es noch eine weitere Rechtsgrundlage für die bisher üblichen Datenübermittlungen in die USA. Das ist etwa der Fall, wenn eine Datenübermittlung erforderlich ist, um einen Vertrag mit einem Kunden ordnungsgemäß zu erfüllen. Dann ist die Übermittlung schon unmittelbar nach der Datenschutz-Grundverordnung zulässig. In diesem Fall kann alles einfach so weiterlaufen wie bisher.
- Ziemlich oft ist es jedoch so, dass der Privacy Shield die einzige rechtliche Basis für die Datenübermittlung in die USA war. Dann muss bildlich gesprochen schnell eine neue Rechtsgrundlage her. Das ist eine große rechtliche Herausforderung.

Enorme Bedeutung für Geschäfte mit den USA

Dies ist der Hintergrund dafür, warum die Datenübermittlungen in die USA in der nächsten Zeit vielleicht auch für Sie ein Thema sein werden. Das kommt im Augenblick sicher ungelegen. Schließlich machen die Corona-Folgen schon genügend Mühe. Das Thema ist aber wichtig, damit unentbehrliche Datenübermittlungen in die USA auch künftig rechtskonform ablaufen können.

2 DATENÜBERMITTLUNG IN DIE USA – WAS BRINGT DIE VERSCHLÜSSELUNG?

Die Datenübermittlung in einen Drittstaat wie die USA ist nur zulässig, wenn dort ein angemessenes Datenschutzniveau sichergestellt ist. Reicht es dazu, die personenbezogenen Daten zu verschlüsseln? Oder ist die Verschlüsselung nur eine Maßnahme von vielen?

Handlungsbedarf bei der Nutzung von Online-Diensten aus den USA

Drei von vier Unternehmen (76 Prozent) nutzten im Jahr 2019 Rechenleistungen aus der Cloud, so die Studie „Cloud-Monitor 2020“ des Digitalverbands Bitkom und der Wirtschaftsprüfungsgesellschaft KPMG. Unternehmen aus Deutschland nutzen Cloud-Dienste aber nicht nur, um Daten zu speichern (Cloud-Storage genannt). Sie verwenden auch Anwendungen aus der Cloud wie Office-Programme, E-Mail-Dienste, Terminverwaltungen, Videokonferenzdienste und Programme zur Datenanalyse, um nur einige Beispiele zu nennen.

Viele Cloud-Dienste werden dabei von Unternehmen aus den USA betrieben. Werden personenbezogene Daten in die Cloud übermittelt, muss es dafür eine Rechtsgrundlage geben, so will es die Datenschutz-Grundverordnung (DSGVO). Bei vielen Cloud-Diensten aus den USA galt bisher der sogenannte „Privacy Shield“ als die Rechtsgrundlage.

Mit dem Urteil des Europäischen Gerichtshofs (EuGH), dass der Privacy Shield als rechtliche Grundlage für die Übermittlung personenbezogener Daten in die USA ungültig ist, stehen viele Unternehmen nun vor einer Herausforderung: Wie können sie nun personenbezogene Daten in einen Cloud-Dienst übertragen, der in den USA betrieben wird?

Von rechtlicher Seite gibt es viele Überlegungen und Hinweise, worauf ein Unternehmen nun achten muss. Gleichzeitig melden sich Anbieter von Verschlüsselungslösungen zu Wort, man könne das Privacy-Shield-Problem lösen, indem man einfach alle Daten verschlüsselt.

So manches Unternehmen denkt nun: Wenn die Daten verschlüsselt sind, kann man sie problemlos in die USA übermitteln, auch wenn Privacy Shield keine Rechtsgrundlage sein kann und es keine andere Rechtsgrundlage gibt. Doch stimmt das?

Nutzung der verschlüsselten Daten in den USA

Ohne in die Tiefen des Datenschutzrechts einzutauchen, lohnt sich bereits die Überlegung, ob die Daten beim Empfänger, also zum Beispiel bei dem Cloud-Betreiber in den USA, verschlüsselt bleiben. Nehmen wir das Beispiel, dass ein Unternehmen einen Cloud-Dienst für Maschinelles Lernen in den USA nutzen möchte, ein häufig anzutreffender Fall.

Zum einen lassen sich die verschlüsselten Daten nicht mittels Maschinellen Lernens verarbeiten und analysieren. Zum anderen muss auch auf dem Server in den USA sichergestellt sein, dass nur Befugte die Daten weiterverarbeiten. Das setzt aber eine Rechtsgrundlage voraus. Ein „Ersatz“ für Privacy Shield ist die Verschlüsselung also nicht.

Personenbezug bei verschlüsselten Daten

Manchmal hört man das Argument, verschlüsselte Daten würden nicht mehr dem Datenschutz unterliegen, denn sie hätten den Perso-

nenbezug verloren. Wäre dem so, könnten verschlüsselte Daten ohne datenschutzrechtliche Vorgaben übermittelt und verarbeitet werden.

Aber Vorsicht: Verschlüsselte Daten sind ein klassisches Beispiel für Pseudonymisierung, so die Aufsichtsbehörden für den Datenschutz. Die verschlüsselten Informationen beziehen sich auf Personen, die durch einen Code gekennzeichnet sind, während der Schlüssel für die Zuordnung des Codes zu den Kennzeichen der Personen (zum Beispiel Name, Geburtsdatum, Adresse) gesondert aufbewahrt wird.

Pseudonyme Daten sind jedoch weiterhin personenbeziehbar. Denn sie lassen sich durch Heranziehung zusätzlicher Informationen einer natürlichen Person zuordnen. Man müsste zuverlässig verhindern können, dass der Cloud-Betreiber in den USA oder andere Stellen dort den Schlüssel zur Entschlüsselung erlangen können. Dann aber könnten die Daten in der Cloud auch nicht weiterverarbeitet werden.
Man kann also nicht davon ausgehen, dass verschlüsselte Daten nicht mehr dem Datenschutz unterliegen. Unternehmen brauchen somit auch für die Übermittlung verschlüsselter Daten eine Rechtsgrundlage.

Allein die Verschlüsselung reicht nicht

Aber auch wenn es nicht ausreicht, die personenbezogenen Daten zu verschlüsseln, um sie in einen Drittstaat wie die USA übermitteln zu dürfen, ist die Verschlüsselung durchaus eine wichtige zusätzliche Maßnahme bei einer Datenübermittlung.

Verschlüsselung gehört zu den zusätzlichen Maßnahmen, um ein Datenschutzniveau sicherzustellen, das dem in der EU gleichgestellt ist, so die Aufsichtsbehörden. Nur dann, wenn ein angemessenes Datenschutzniveau im Empfängerland bei der Übermittlung personenbezogener Daten sichergestellt ist, darf die Datenübermittlung erfolgen. Nur dann also dürfen Unternehmen Online-Dienste aus den USA weiterhin nutzen, wenn damit personenbezogene Daten verarbeitet werden sollen. Die Verschlüsselung allein reicht dafür nicht, auch wenn dies manche Anbieter behaupten. Es gilt nun besonders, Angebote zu hinterfragen, die technische Lösungen zum Privacy-Shield-Problem offerieren.

3 VIDEOÜBERWACHUNG VON BAUSTELLEN

Es gibt viele gute Gründe, eine Baustelle mit Video zu beobachten. Das sehen die Datenschutzgesetze ebenfalls so. Aber auch Bauarbeiter haben Persönlichkeitsrechte. Sie gilt es zu beachten.

Möglicher Zweck einer Überwachung

Eine Videoüberwachung von Baustellen kann unterschiedliche Gründe haben:

- Manchmal will der Bauherr im Internet zeigen, wie gut es auf der Baustelle vorangeht. Das zieht vielleicht zahlungskräftige Käufer oder Mieter an.
- Meist geht es aber darum, Diebstähle zu verhindern. Auf Baustellen findet sich viel wertvolles Material. Das lockt manchmal völlig falsche Interessenten an.
- Relativ oft spielt auch der Schutz vor Vandalismus eine Rolle. Viel zu oft verwirklichen sich zweifelhafte „Künstler“ auf gerade fertiggestellten Fassaden.

Unterschiedliche Arten von Aufnahmen

Mit diesen Stichworten ist der Zweck einer Videoüberwachung beschrieben. Er bestimmt, welche Art von Aufnahmen erforderlich ist:

- Um die Fortschritte auf der Baustelle stolz im Internet zu zeigen, genügen Panorama-Aufnahmen der gesamten Baustelle. Einzelne Personen müssen auf ihnen nicht zu erkennen sein. Sie interessieren nicht.
- Anders sieht es aus, wenn es um den Schutz vor Diebstählen oder Vandalismus geht. Dann soll die Videoaufnahme im Ernstfall als Beweismittel dienen. Sie geht dann an die Polizei, um die Täter zu finden.

Zusammenhang von Zweck der Überwachung und Art der Aufnahme

Der Zweck der Videoüberwachung bestimmt somit, welche Art von Aufnahme erlaubt ist. Aber auch die Interessen der Bauarbeiter kommen ins Spiel. Um ihre Arbeit zu erledigen, müssen sie während ihrer gesamten Arbeitszeit auf der Baustelle präsent sein und sich dort bewegen.

Persönlichkeitsrechte der Bauarbeiter

Wie für alle anderen Arbeitnehmer gilt auch für sie: Eine ständige Videoüberwachung ist normalerweise nicht zulässig. Natürlich könnte es auch vorkommen, dass ein Bauarbeiter während seiner Arbeit einen Diebstahl begeht. Das ist jedoch die Ausnahme.

Deshalb bleibt es bei der Grundregel, die auch sonst im Arbeitsleben gilt: Um Diebstähle durch Beschäftigte aufzuklären, ist eine Videoüberwachung erst zulässig, wenn zuvor alle anderen Mittel ausgeschöpft wurden. Eine rein vorbeugende Videoüberwachung, um Diebstähle durch Beschäftigte zu verhindern, wäre nicht zulässig.

Typische Faustregeln

Berücksichtigt man diese Hintergründe, kristallisieren sich einige einfache Faustregeln für die Videoüberwachung von Baustellen heraus. Sie lauten:

- Im Regelfall ist eine Videoüberwachung nicht während der Zeiten zulässig, in denen auf der Baustelle gearbeitet wird.
- Wird nur auf einem Teil der Baustelle gearbeitet, können die anderen Teile der Baustelle aber überwacht werden.
- Die Videoüberwachung darf nur die Baustelle selbst erfassen. Nachbargrundstücke und öffentliche Straßen vor der Baustelle sind tabu. Wenn Diebe über ein Nachbargrundstück auf die Baustelle kommen könnten, ist ein ordentlicher Zaun das richtige Mittel dagegen, nicht jedoch die Videoüberwachung des Nachbargrundstücks.

Informationspflichten

Selbstverständlich gelten auf Baustellen dieselben Informationspflichten für die Datenverarbeitung wie sonst auch. Notwendig sind deshalb klare und deutliche Hinweisschilder. Sie müssen die üblichen Angaben enthalten. Insbesondere müssen sie Auskunft darüber geben, wer für die Videoüberwachung verantwortlich ist.

Klärung der Verantwortung

Diese Frage ist nicht immer einfach zu beantworten. Oft gibt es einen Generalunternehmer, der alle Abläufe auf der Baustelle koordiniert und betreut. Dann wird normalerweise er der Verantwortliche sein. Denkbar ist aber auch, dass unterschiedliche Unternehmen für verschiedene Bereiche der Baustelle die Verantwortung tragen. Dann gibt es für unterschiedliche Baustellenabschnitte unterschiedliche Verantwortliche.

Abschreckung? Gern!

Manche meinen, dass solche Hinweisschilder auf Diebe und andere unliebsame Besucher abschreckend wirken. Das ist dann ein willkommener Nebeneffekt, der aber mit dem Datenschutz nichts zu tun hat.

Löschung der Videoaufnahmen

Nach welcher Zeit die Videoaufnahmen gelöscht werden müssen, lässt sich nicht pauschal beantworten. In der Regel sollte es möglich sein, Aufnahmen binnen zweier Wochen auszuwerten. Praktisch sind Kamerasysteme, die gar keine längeren Aufzeichnungen zulassen.

Nach spätestens zwei Wochen werden die alten Aufnahmen durch neue Aufzeichnungen überschrieben.

Das gilt selbstverständlich nur, wenn nichts vorgefallen ist. Kam es dagegen etwa zu einem Diebstahl, stellt der Verantwortliche die Aufnahmen sicher und übergibt sie der Polizei.

4 WAS IST WIRKSAMER DATENSCHUTZ?

Es reicht nicht, wenn man möglichst viele Datenschutz-Maßnahmen ergreift, die dann aber letztlich nicht funktionieren. Datenschutz muss wirksam sein, sonst ist er nur gut gemeint, aber nicht gut gemacht. Und von dieser Wirksamkeit muss man sich überzeugen.

Viel ist getan, nichts hat geholfen

Stellen Sie sich vor, Ihr Unternehmen hätte bei verschiedenen Gelegenheiten Gewinnspiele veranstaltet und dabei personenbezogene Daten der Teilnehmer erhoben, darunter die Kontaktdaten. Diese Daten wollte Ihr Unternehmen auch zu Werbezwecken einsetzen, vorausgesetzt natürlich, die Teilnehmerinnen und Teilnehmer hätten hierzu ausdrücklich und informiert eingewilligt.

Um zu verhindern, dass Personen, die nicht eingewilligt haben, nach der Gewinnspiel-Teilnahme Werbung zugeschickt bekommen, hat Ihr Unternehmen verschiedene technische und organisatorische Maßnahmen ergriffen. Unter anderem hat es spezielle Richtlinien erstellt und Schulungen abgehalten.

Trotzdem bekommen auch solche Teilnehmer Werbung, die gar nicht eingewilligt haben. Offensichtlich haben die Datenschutz-Maßnahmen nicht gegriffen. Das ist nicht nur ein theoretisches Beispiel, es passiert in der Praxis.

Datenschutz war nicht wirksam

All die Datenschutz-Maßnahmen konnten nicht verhindern, dass die Daten zweckentfremdet wurden. Ohne jede Einwilligung wurden die Kontaktdaten zu Werbezwecken verwendet. Man muss feststellen: Der Datenschutz war nicht wirksam. Das sollte sich aber nicht erst durch eine solche Datenschutzverletzung und Beschwerden Betroffener zeigen. Das muss ein Unternehmen frühzeitig selbst feststellen.

So fordert die Datenschutz-Grundverordnung (DSGVO) ausdrücklich „ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“.

Kommt es trotz Datenschutz-Maßnahmen zu einer Datenpanne, wie in dem beschriebenen Fall, dann kann man davon ausgehen, dass es kein solches Verfahren gibt – jedenfalls keines, das funktioniert. Das kann dann dazu führen, dass eine Aufsichtsbehörde ein Bußgeld verhängt oder zu anderen Sanktionen greift.

Datenschutz überprüfen und testen

„Datensicherheit ist eine Daueraufgabe“, betont zum Beispiel der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Dr. Stefan Brink. „Technische und organisatorische Maßnahmen sind regelmäßig den tatsächlichen Verhältnissen anzupassen, um auf Dauer ein angemessenes Schutzniveau sicherzustellen.“

In der Praxis bedeutet das: Unternehmen müssen die Maßnahmen im Datenschutz auf Erfolg und Wirksamkeit hin überprüfen. Richtlinien zum Datenschutz müssen also nicht nur defi-

niert, geschult und eingeführt werden, sie müssen auf Wirksamkeit hin überprüft und im Fall des Falls überarbeitet werden. Dazu gehört es insbesondere, alle Maßnahmen, die sich nicht praktisch verwirklichen lassen, durch andere, wirksame Maßnahmen zu ersetzen, die eine Praxisprobe bestehen.

Hier sind alle gefordert, auf den Erfolg von Datenschutz-Maßnahmen zu achten. Es darf nicht so sein, dass Beschäftigte Datenschutz-Maßnahmen einfach nur als praxisfremd abtun und nicht beachten. Vielmehr sollten Sie auf mögliche Probleme hinweisen, wenn Ihnen Abweichungen im Datenschutz auffallen, die auch dadurch entstehen können, dass gut gemeinte Maßnahmen nicht greifen.

Ist der Datenschutz wirksam? Machen Sie den Test!

Wenn Datenschutz-Maßnahmen realitätsfremd erscheinen, braucht man sie nicht einzuhalten. Stimmt das?

1. Nein, aber man sollte auf seine Bedenken hinweisen.
2. Ja, denn solche Maßnahmen bringen sowieso nicht für den Datenschutz.

Lösung:

Die Antwort 1. ist richtig. Wie bei jeder betrieblichen Vorgabe müssen Sie auch die betrieblichen Datenschutzrichtlinien beachten, selbst wenn sich der Sinn vielleicht nicht sofort erschließt oder Sie meinen, dieses oder jenes bringe nichts. Wenn Ihnen Probleme bei Maßnahmen auffallen, melden Sie das. Lassen Sie aber nicht ohne Weiteres die Vorgaben unbeachtet.

Bekannte Datenschutz-Maßnahmen wie Verschlüsselung sind immer wirksam. Stimmt das?

1. Ja, sonst würden nicht so viele Unternehmen sie nutzen.
2. Nein, man muss auch solche Maßnahmen regelmäßig auf Erfolg überprüfen.

Lösung:

Die Antwort 2. ist richtig. Maßnahmen wie Verschlüsselung sind zwar seit vielen Jahren praxiserprobt, doch ob sie den gewünschten Schutz bringen, muss in jedem Einzelfall geklärt werden. So kann es sein, dass die Verschlüsselung nicht alle zu schützenden Daten umfasst, die Verschlüsselung nicht mehr dem Stand der Technik entspricht oder der Schlüssel zur Entschlüsselung unsicher aufbewahrt wird, um nur einige Beispiele zu nennen. Die Wirksamkeit auch solch bekannter Maßnahmen wie Verschlüsselung personenbezogener Daten muss geprüft werden, sonst könnte nur eine Scheinsicherheit vorliegen. Eine Datenschutzverletzung könnte die Folge sein.

IMPRESSUM

Redaktion
Dr. Uwe Günther
Sanovis GmbH
Richard-Strauss-Straße 69
81679 München
089-99 27 579 22
Uwe.Guenther@Sanovis.com

Stefan Strüwe, RA
CURACON GmbH Wirtschaftsprüfungsgesellschaft
Am Mittelhafen 14
48155 Münster
02 51-92 208 209
Stefan.Struewe@Curacon.de