Antworten der Referenten Katharina Raabe-Stuppnig und Armin Simon auf Fragen der Teilnehmer, die während der Live-Sendung aus Zeitgründen nicht beantwortet werden konnten:

(chronologisch aufgeführt; alle Fragen im Original-Wortlaut)

Frage 1:

Kann ich als Betroffener in Bezug auf meinen Auskunftsanspruch vom Verarbeiter verlangen, mir die abgeschlossenen SCCs zwischen dem Verarbeiter und dem Cloud-Provider zu offenbaren? Meines erachtens wird oft nur Behauptet, es ist alles konform. Aber welche Rechte habe ich, um wirklich einen Nachweis ansatt nur eine schwammige Aussage zu bekommen?

Antwort von Frau Raabe-Stuppnig:

Laut Durchführungsbeschluss der Kommission haben die Parteien der betroffenen Person auf Anfrage eine Kopie dieser Klauseln unentgeltlich zur Verfügung zu stellen (einschließlich der von ihnen ausgefüllten Anlage). Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten, notwendig ist, können die Parteien Teile des Textes der Anlage vor der Weitergabe einer Kopie unkenntlich machen; sie legen jedoch eine aussagekräftige Zusammenfassung vor, wenn die betroffene Person andernfalls den Inhalt der Anlage nicht verstehen würde oder ihre Rechte nicht ausüben könnte. Auf Anfrage teilen die Parteien der betroffenen Person die Gründe für die Schwärzungen so weit wie möglich mit, ohne die geschwärzten Informationen offenzulegen.

Frage 2:

Gibt es von Microsoft vorgefertigte SCC die man abschließen kann?

Antwort von Frau Raabe-Stuppnig:

Es gibt den von der Kommission vorgegeben vertraglichen Text, der abgeschlossen werden kann. Zusätzlich müssen aber die Anhänge beachtet und abgeschlossen werden. Hier kommt es darauf an, dass die Anhänge (insb. die TOM) dem Einzelfall angemessen das Datenschutzniveau gewährleisten. Es ist nicht ausreichend, sich lediglich auf (Werbe-)Aussagen zu verlassen.

Frage 3:

Ist es eigentlich ok, dass z.B. Google die Informationen (nur) auf Englisch herausgibt? Die bieten Ihre Dienste doch auf dem deutschen Markt an, müssen diese Bedingungen nicht auch auf deutsch sein?

Antwort von Frau Raabe-Stuppnig:

Im Sinne des Verbraucherschutzes müssten die Informationen den Betroffenen auch auf Deutsch zur Verfügung gestellt werden. Hinsichtlich der (Unternehmens-)Vertragspartner kann man Englisch als Vertragssprache wählen.

Frage 4:

wenn ich als SaaS Provider Data Processor für Personenbezogene Daten von meinen Kunden bin und Google als Sub-Processor nutze, wer kann/muss dann die Externen Encryption Keys halten: ich als SaaS Provider oder der Kunde?

Antwort von Frau Raabe-Stuppnig:

Wichtig ist, dass der Schlüssel extern (beim Kunden oder bei einem Treuhänder) gehalten wird, um dem Zero-Knowledge-Prinzip gerecht zu werden.

Frage 5:

Aus meiner Sicht ist dies auch in Europa eine Information des Auftraggebers nicht möglich, wenn dies aufgrund Ermittlungstaktischer Gründen untersagt wird. Wo liegt da genau der Unterschied zum Europäischen Recht?

Antwort von Frau Raabe-Stuppnig:

Europäisches Überwachungsrecht ist in Zusammenhang mit den SCC nicht relevant. Es geht um die Gewährleistung des Datenschutzniveaus bei Datenexport aus der EU in ein Drittland und das damit verbundene Risiko.

Frage 6:

ca 5000 Anfragen davon ca 7000 Accounts ????

Antwort von Herrn Simon:

Das war bei den Law Enforcement Reports von Microsoft: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

Offensichtlich kann eine Anfrage mehrere Accounts betreffen. Die Möglichkeit, Informationen zu den Behördenanfragen aufzudecken, sind sehr eingeschränkt, wodurch die Cloud-Anbieter nur aggregierte Daten zweimal jährlich veröffentlichen.

Frage 7:

Was hilft denn eine technisch hochwertige Verschlüsselung und Schlüsselhoheit, wenn Geheimdienste wie z.B. die NSA technisch in der Lage sind, Verschlüsselungen zu

"knacken" (auch im Kontext Quanten-Computing interessant)? Ist die EU da nicht sehr blauäuig und realitätsfremd?

Antwort von Herrn Simon:

Sauber implementierte Verschlüsselung funktioniert und gilt weiterhin als sicher. Die Snowden-Veröffentlichungen haben gezeigt, dass Verschlüsselung eines der wenigen Dinge ist, auf die man sich verlassen kann.

Es wird allerdings erwartet, dass Quantencomputer zur Bedrohung für bestimmte asymmetrische Verschlüsselungsverfahren werden. Dies wird, nach einhelliger Expertenmeinung, nicht vor 2030 der Fall sein und auch dann „nur“ für einzelne Schlüssel in wochen- bzw. monatelangen Aufwand zu brechen sein. Abhilfe bieten quantensichere Verfahren, welche sich bereits im Standardisierungsverfahren befinden. Weiterführender Artikel zum Thema: https://www.heise.de/news/BSI-Leitfaden-soll-bei-quantensicherer-Verschluesselung-helfen-6296863.html

Frage 8:

Ergänzung: Ionic sowie Fortanix als External Key Manager sind ebenfalls US-Unternehmen

Antwort von Herrn Simon:

Die Ergänzung bezieht sich auf die Supported Partners für Google EKM https://cloud.google.com/kms/docs/ekm#supported_partners

Die Google Cloud Platform (GCP) setzt auf mehrere Anbieter. GCP bedient einen globalen Markt und US-Anbieter werden auch ihre Marktberechtigung haben.

Frage 9:

Herr Simon war unsicher, warum MS schreibt, dass MS die neuen SCCs "abgeschlossen" hätte --> Vielleicht war hiermit der Abschluss von SCCs zwischen MS Ireland und MS Corp./USA gemeint.

Antwort von Frau Raabe-Stuppnig:

Das ist möglich und ist ein guter erster Schritt. Im Ergebnis kommt es für den Verantwortlichen (den Auftraggeber) aber darauf an, dass das Datenschutzniveau gewährleistet bleibt und dafür reicht der Abschluss von SCC alleine nicht aus. Insb. durch die individuellen Anhänge muss das Zero-Knowledge-Prinzip sichergestellt werden.

Frage 10:

Was bedeutet das für die Nutzung von Services amerikanischer Anbieter wie z.B. O365, MS Teams, Google Docs deren Daten auf europäischen Servern liegen? Hier kann ich als

Nutzer keine zusätzlichen Maßnahmen setzen, da ich die Services nicht betreibe. Wäre daher die Folge, dass diese Services in Europa nicht mehr genutzt werden dürfen?

Antwort von Frau Raabe-Stuppnig zu Teil 1 der Frage:

Aufgrund des Weisungsrechts der amerikanischen Konzernmutter muss die europäische Tochtergesellschaft die Daten, die bei ihr liegen, rausgeben. Das ist dann nicht problematisch, wenn die Daten verschlüsselt sind und der Schlüssel extern – dh nicht bei der Tochter – gehalten wird. Dann kann die Tochter nur verschlüsselte Daten herausgeben.

Antwort von Herrn Simon zu Teil 2 der Frage:

Auch wenn der Service nicht durch Sie betrieben wird, gibt es in bestimmten Fällen die Möglichkeit für zusätzliche Maßnahmen. Das ist Thema für den Webcast am 24.02.22: https://business-services.heise.de/security/datenschutz-dsgvo/beitrag/das-schrems-ii-urteil-und-dessen-folgen-wie-erreiche-ich-konformitaet-bei-den-hyperscalern-4213

Frage 11:

Kurz gesagt: SSC mit Processor in den US ist nur möglich, wenn 0-Knowledge-Prinzip oder vergleichbares implementiert ist. Habe ich das richtig verstanden?

Antwort von Frau Raabe-Stuppnig:

Ja.

Frage 12:

An beide Referenten: Herzlichen Dank für die spannenden Eindrücke. Gibt es Neuigkeiten zu den TIAs zwischen Datenexporteuren und Datenimporteuren - also etwa zw. Microsoft Irland und MS USA (oder Google oder AWS oder...)?

Antwort von Frau Raabe-Stuppnig:

Es gibt die neuen Leitlinien 05/2021 des EDSA, vielleicht hilft dieser Link: https://www.dr-datenschutz.de/drittlanduebermittlung-leitfaden-zu-transfer-impact-assessments/

Frage 13:

Wie ist die Verwendung von SaaS (z.B. Workday, SAP Sales Cloud) im Kontext von Schrems II zu sehen?

Antwort von Herrn Simon:

Schutzmaßnahmen – das ist das Thema für den Webcast am 24.02.22:

https://business-services.heise.de/security/datenschutz-dsgvo/beitrag/das-schrems-ii-urteil-und-dessen-folgen-wie-erreiche-ich-konformitaet-bei-den-hyperscalern-4213

Frage 14:

Müssen denn jetzt alle Kleine- und Mittelständischen Unternehmen für JEDE Nutzung amerikanischer Anbieter sei es für Cloud Dienste, Social Media Dienste, Microsoft Anwendungen etc. dieses Procedere Standardvertragsklauseln und zusätzliche Maßnahmen durchziehen?

Antwort von Frau Raabe-Stuppnig:

Ja.

Frage 15:

Wenn ein Mitarbeiter in Deutschland eine Mail an einen Partner in China schickt - ist das schon ein Datentransfer in ein Drittland? Dasselbe für den Mitarbeiter, der eine Mail nach Kanada schickt, die über die USA geroutet wird. Danke ;-)

Antwort von Frau Raabe-Stuppnig:

Kommt darauf an, was in der Mail drinnen steht. Sobald personenbezogene Daten enthalten sind, handelt es sich um einen Datentransfer in ein Drittland, der eventuell als Einzelfall iSd Ausnahme nach Art 44ff DSGVO zu qualifizieren ist (einzelne Flugbuchung/Hotelbuchung). Sobald personenbezogene Daten strukturiert in Drittländer geschickt werden, braucht man SCC.

Frage 16:

Wie geht man mit dem Verschicken von Dumps an die Hersteller um, wo die personenbezogenen Daten nicht anonymisiert werden können? Die deutsche Datenschutzkonferenz hat das als Auftragsverarbeitung definiert (Bsp. Softwarewartung von Oracle, Microsoft usw.). Verschlüsseln macht hier keinen Sinn.

Antwort von Herrn Simon und Frau Raabe-Stuppnig:

Memory Dumps können personenbezogene Daten enthalten. Es ist bestimmt auch eine Frage, welche Daten es sind und somit genauer zu klären. Besteht eventuell ein Einzelfall iSd Ausnahme nach Art 49 DSGVO, möglicherweise „Erwägungsgrund 113 Nicht wiederholend erfolgende und nur eine begrenzte Zahl von Betroffenen betreffende Übermittlungen“.

Sobald eine strukturierte Verarbeitung stattfindet, kommt das allerdings nicht mehr infrage. Wenn eine Verschlüsselung nicht möglich ist, liegt es am Verantwortlichen, zu entscheiden, ob er die Daten dennoch schickt und welche Sicherheitsvorkehrungen getroffen werden können. Selbst wenn eine Verschlüsselung nicht infrage kommen sollte, können andere ergänzende Maßnahmen (Pseudonymisierung, Datenminimierung etc) ergriffen werden. Ob diese dann im Einzelfall ausreichen, um das Datenschutzniveau zu gewährleisten, wird man erst wissen, wenn die Behörde darüber entschieden hat. Es ist aber jedenfalls von Vorteil,

wenn man der Behörde dokumentiert begründen kann, warum man zu der Auffassung gelangt ist, dass ein Übermitteln der Daten in das Drittland das Datenschutzniveau nicht gefährdet. Je mehr Argumente man ins Treffen führen kann, desto besser. Es ist und bleibt aber eine Risikoentscheidung.

Frage 17:

Die österreichische Datenschutzbehörde ist nachweislich ein zahnloser Tiger, der nicht beißt, wie einige Gerichtsurteile gezeigt haben (u.a. A1 Telekom). Da braucht sich niemand fürchten.

Antwort von Frau Raabe-Stuppnig:

Die europäischen Aufsichtsbehörden gehen bei Verstößen gegen die DSGVO hart vor. Die Höhe der Strafen geht in die Millionen, auch viele Firmen in Österreich sind betroffen. Europaweit wurden bereits laut dem DSGVO-Report 2020 272,5 Millionen Euro Bußgeld verhängt und die Höhe steigt jährlich. In Österreich wurde zuletzt im September 2021 eine Strafe von EUR 9,5 Mio gegen die Post verhängt (nicht rechtskräftig). Österreich tendiert auch zu einer strengen Handhabung von Schrems II Verstößen – siehe Entscheidung „google analytics“ https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_DE_bk_0.pdf

Frage 18:

Also werden die Daten für die Verarbeitung weiter entschlüsselt und können dann von den Plattformbetreibern wofür auch immer verwendet werden (die Zusicherung können weder überprüft werden noch Verstöße eingeklagt werden) bzw. durch die Behörden abgegriffen werden. D. h. die Plattformen können höchstens zur Datenspeicherung benutzt, aber nicht für die Funktionen der Plattformen (soweit es sich um personenbezogene Daten handelt). Richtig?

Antwort von Herrn Simon:

In dem Moment, in dem Daten verarbeitet werden, müssen sie unverschlüsselt sein*. Das European Data Protection Board (EDPB) fordert allerdings „nur“ die Verschlüsselung der gespeicherten Daten und die vollständige Kontrolle über das Schlüsselmaterial. Bei der Verarbeitung werden temporär einzelne Datensätze im Arbeitsspeicher zur Verarbeitung entschlüsselt verfügbar gemacht.

Auch wenn die Latte deutlich höher liegt, ist ein Angriff auf dieser Ebene durchaus denkbar. Angriffe auf einzelne Datensätze im Arbeitsspeicher sind allerdings sehr aufwändig und eignen sich daher kaum für massenhaften Datenabfluss. Auch das gezielte Abfragen von Daten wird nahezu unmöglich. Es gibt das Beispiel der Steuer-CDs bei den Schweizer Banken. Die Verschlüsselung der Daten, bei getrennter unkopierbarer Aufbewahrung des Schlüsselmaterials, hätte diesen Datenabfluss verhindert.

*THALES bietet auch Lösungen für Confidential Computing, welche spezielle CPU-Fähigkeiten zum Schutz während der Datenverarbeitung nutzen (z.B. in Verbindung mit Google Ubiquitous Data Encryption). https://cpl.thalesgroup.com/blog/encryption/google-ubiquitous-data-encryption-ekm

Frage 19:

Aber Anbieter, welche Ihre Dienstleistungen in Europa Anbieten müssen sich doch an die DSGVO halten? Das tuen doch die Clouddienstleister. Auch ohne dass ein Unternehmen diesen nutzt.

Antwort von Frau Raabe-Stuppnig:

US-Unternehmen müssen gemäß Cloud Act Daten an Behörden herausgeben. Daher müssen in den neuen SCC in Anhang II TOMs zum Schutz der personenbezogenen Daten vereinbart werden, welche den Zugriff verhindern.

Frage 20:

Eine Nutzung von MS365 ist doch nach diesen Informationen für Europäer überhaupt nicht mehr möglich?!

Antwort von Herrn Simon:

Nicht ohne zusätzliche Schutzmaßnahmen. TOMs für M365 sind aktuell eine der größeren Hürden. Derzeitige Ansätze sind Gateway-Lösungen oder Nutzung und Kontrolle des MS-Schlüsselmaterials. Weitere Details im nächsten Webcast am 24.02.22:

https://business-services.heise.de/security/datenschutz-dsgvo/beitrag/das-schrems-ii-urteil-und-dessen-folgen-wie-erreiche-ich-konformitaet-bei-den-hyperscalern-4213

Frage 21:

Im Kontext von Art. 27 DSGVO sollte es schon einen Vertreter geben ... https://www.datenschutzexperte.de/gesetzestext-eu-dsgvo/artikel-27/

Antwort von Frau Raabe-Stuppnig:

Nur in speziellen Fällen und selbst wenn es einen Vertreter gibt, befreit dies nicht von den sonstigen Sorgfaltspflichten des Verantwortlichen.

Frage 22:

Wie machen Sie die SCC mit Microsoft zu Office 365? Aktuell müssten die Aufsichtsbehörden eigentlich alle Verarbeitungen mit Office untersagen. Trotzdem gehen immer mehr Unternhemen zu Office 365.

Antwort von Herrn Simon:

Siehe Antwort zu Frage 20.

Frage 23:

Wenn jeder mit MS einen eigenen Vertrag auf basis der SCC machen muss, macht a) MS das mit und b) gibt es nicht noch mehr Unsicherheit und unkorrekte Verträge? Wie sind die DPAs von MS als Umsetzung der SCCs zu bewerten?

Antwort von Frau Raabe-Stuppnig:

Die Verantwortlichen sind dazu berufen sicherzustellen, dass das Datenschutzniveau gewährleistet bleibt. Der SCC-Text wird sich nicht ändern – eine Abänderung der Klauseln wäre gar nicht zulässig, aber die SCC alleine sind nicht ausreichend, sondern über die in den Anhängen definierten ergänzenden Maßnahmen muss das Datenschutzniveau faktisch gewährleistet werden. Das muss insb. über die TOM passieren. Wenn MS standardisiert eine ausreichende Verschlüsselung (externes Key Management) anbietet, kann dieses in Anspruch genommen werden und die Verträge müssen nicht jedes Mal im Einzelnen verhandelt werden. Solange das noch nicht der Fall ist, liegt es am Verantwortlichen. zu prüfen und zu dokumentieren, warum das Datenschutzniveau gewährleistet bleibt, auch wenn die Daten aus der EU exportiert werden.

Siehe auch: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

Frage 24:

Gibt es für die neuen SCC ein Tool, mit dem man diese Teile / Optionen zusammensetzen kann?

Antwort von Frau Raabe-Stuppnig:

Nein.

Frage 25:

Bis auf Google scheint es heute gar nicht möglich zu sein z. B. mit Microsoft alle relevanten TOMs zu ergreifen. Kann dann die MSFT Cloud überhaupt Schrems II konform eingesetzt werden?

Antwort von Herrn Simon:

An bestimmten Stellen ist es eine größere Herausforderung (siehe auch Frage 20). An anderen Stellen gibt es gute Möglichkeiten, TOMs zu implementieren. Weitere Details im nächsten Webcast am 24.02.22:

https://business-services.heise.de/security/datenschutz-dsgvo/beitrag/das-schrems-ii-urteil-und-dessen-folgen-wie-erreiche-ich-konformitaet-bei-den-hyperscalern-4213

Frage 26:

Bei der Anwendung der neuen SDK werden teilweise auch mehrere Module angewandt. Z.B.: verlangt Zoom die Modulteile 1,2,3 weil die unterschiedlichen Datentransfers trennt. Die pb Daten zur Abwicklung des Geschäftes (Kunde gibt Daten der Kontaktpersonen für die Lizenz und die Bezahlung) werden mit Modul 1 abgedeckt. Die Daten zur Nutzung der Kommunikationsplattform Zoom des Kunden werden mit Modul 3 abgedeckt.

Antwort von Frau Raabe-Stuppnig:

Ja, es kann durchaus sein, dass mehrere Rollen abgedeckt werden müssen, dann braucht man die jeweiligen Module.

Frage 27:

Wenn wir die Schlüssel nicht für den Cloud Provider zugänglich machen dürfen (was ja Sinn macht), dann dürfen diese auch nicht in der Cloud für Services (Programme) geladen werden. Somit kann man IN der Cloud auch nicht mit diesen Daten arbeiten. Dann reduziert sich die Cloud faktisch zum reinen exteren Cloud Storrage.

Antwort von Herrn Simon:

Ja, auch der Europäische Datenschutzausschuss weist darauf hin, dass US-Datenimporteure direkt verpflichtet sind, Zugang zu importierten personenbezogenen Daten zu gewähren und dass sich dies auch auf alle kryptografischen Schlüssel erstrecken kann, die erforderlich sind, um die Daten verständlich zu machen.
Aber es gibt durchaus Möglichkeiten, Cloud-Daten zu verschlüsseln und das Schlüsselmaterial extern zu halten. Siehe auch Antwort zu Frage 18.

Frage 28:

Ohne die Schlüssel in die Cloud zu laden, wären dann alle Software as a Service (SaaS) Services faktisch nicht Datenschutzkonform, sobald man auch nur einen einzigen personenbezogenen Bezug (Benutzernamen, Anmeldenamen, Customer-ID) in der Cloud verwendet. Und sei es nur zu Anzeige auf der Web-Oberfläche oder zur Anmeldung?!

Ja, es handelt sich um personenbezogene Daten. Bereits hier besteht das Problem.

Frage 29:

wie kann ich beispielsweise meine Stadtverwaltung konkret auf Ihre Verpflichtungen in diesem Zusammenhang hinweisen und auch verpflichtend zur Einhaltung bewegen. Inhalte werden dort häufig z.B. über youtube bereitgestellt...

Antwort von Frau Raabe-Stuppnig:

Sie schriftlich auf die Verfehlung hinweisen und darauf, dass die Datenschutzbehörde informiert werden muss, wenn weiterhin das Schutzniveau personenbezogener Daten gefährdet scheint.

Frage 30:

Kann mit SSC (allgemeinen (EU) oder bilateral unter Unternehmen abgeschlossene) US-Bundesrecht (Cloud-Act) außer Kraft gesetzt werden? Personenbezogene Daten dürfen in unsichere Drittstatten exportiert werden, sobald die "sicher" verschlüsselt wurden? -> Zero Knowledge

Antwort von Frau Raabe-Stuppnig:

Es handelt sich um einen Vertrag, der zwischen den Parteien abgeschlossen wird. Dh. die Vertragsparteien verpflichten sich wechselseitig dazu, die Regeln einzuhalten. Um das „Over Ruling“ durch US-Recht nicht infrage zu stellen, muss verschlüsselt werden.

Frage 31:

Im Zuge einer großen Multi-Cloud Anwendung habe ich mich als Mutli-Tenancy Software Architekt vor allem mit der Tenant-speziefischen Verschlüsselung (teils per HKS) beschäftigt, man kann jedoch nicht vollständig verhindern, da die Cloud Anbieter jederzeit in die Netzwerk Kommunikation Einblick haben.

Antwort von Herrn Simon:

Diese Frage muss genauer spezifiziert werden. Was ist mit HKS gemeint? Hitachi Kubernetes Service? Gut möglich, dass dort Verschlüsselung mit eigenem Key Manager zu etablieren ist. Sind die Daten auf Anwendungsebene verschlüsselt, ist der Schutz entsprechend auch auf Netzwerkebene gegeben.