RUHR-UNIVERSITÄT BOCHUM

RUB

RUBinform

Datenschutz & Datensicherheit

Newsletter 01|21

IN DIESER AUSGABE:

LINKS ZU DEN BEITRÄGEN:

www.rub.de/rubinform

ZUALLERERST

Liebe Leserinnen und Leser,

ob in der Online-Lehre oder beim mobilen Arbeiten – wir haben das digitale Miteinander schätzen gelernt. Dennoch zeigen der letztjährige Cyber-Angriff und andere Ereignisse die Verletzlichkeit unserer Systeme. Schwachstellen in IT-Systemen, organisatorische Defizite oder menschliche Unachtsamkeit gefährden leicht die Funktionsfähigkeit großer Bereiche. Die RUB hat daher begonnen, die zentrale IT nach der IT-Grundschutz-Methodik abzusichern. In weiteren Schritten soll diese Methodik auch auf dezentrale IT-Systeme angewandt werden. Von Synergien aus Datenschutz, VVT und IT-Grundschutz werden dabei alle profitieren.

Die Stabsstellen für Informationssicherheit und Datenschutz wünschen Ihnen einen sicheren Sommer.

CYBERANGRIFF AUF DIE RUB – ALLES WIEDER GUT?

Zunächst ein Rückblick: Am 7. Mai letzten Jahres wurde die Ruhr-Universität Bochum Opfer eines gezielt durchgeführten Cyberangriffs. Direkt nach Feststellung wurden alle windowsbasierten Serversysteme heruntergefahren, um das Ausbreiten der Verschlüsselungsaktivitäten einzudämmen. Die Analyse ergab, dass ca. 60 Serversysteme verschlüsselt wurden. Darunter elementar wichtige Systeme, wie das Active Directory der Ruhr-Universität Bochum, Exchange, SharePoint und zentrale Datenbanken. In der Auswirkung waren große Teile des Campus und der Verwaltung somit arbeitsunfähig, da E-Mail-Kommunikation, Terminierung und Dateizugriffe nicht verfügbar waren. Zentrale Systeme der Personal-, Studierenden- und Finanzverwaltung waren betroffen.

Nach dem Angriff wurde schnellstmöglich ein Notbetrieb eingeleitet, eine Kommunikationsstrategie zur Informationsversorgung entwickelt

©iStock.com/erhui1979

sowie die Bereinigung und der Wiederaufbau der betroffenen Systeme angegangen. Circa acht Wochen nach dem Angriff konnte der Regelbetrieb wiederaufgenommen werden. Entscheidend für diese schnelle Wiederherstellung waren die zu Rate gezogenen Experten, die sehr gute Zusammenarbeit mit der Hochschulleitung sowie die enorme Leistungsbereitschaft der Mitarbeiterinnen und Mitarbeiter. Der Vorfall wurde den Ermittlungsbehörden gemeldet. Ein Lösegeld wurde nicht gezahlt.

Wie sieht es heute aus?

Cybercrime ist weltweit ein milliardenschweres Geschäft. Aus dieser Tatsache und den eigenen Erfahrungen leitet sich die Erkenntnis ab, dass die Bedrohungslage eher weiter zu- als abnimmt. Expert*innen sind sich einig: ein erneuter Angriff lässt sich nicht verhindern. Die Strategie für die RUB muss es daher sein, mögliche Angriffszugänge weiter zu reduzieren und im erneuten Angriffsfall die jeweiligen Auswirkungen davon zu minimieren.

Konkrete Maßnahmen wurden umgesetzt, bzw. befinden sich in der Umsetzung: So wurde ein neues Betriebskonzept mit „Brandschutzabschnitten“ für das Active Directory der RUB eingeführt. Dadurch können die Auswirkungen eines erneuten Angriffs lokaler gehalten werden. Daneben wurde ein neues Konzept zur Verwendung von Administrations-Accounts eingeführt. Die Einführung der neuen Sophos Endpoint Protection wurde vorangetrieben. Organisatorisch wurde gemäß den Vorgaben des Ministeriums für Kultur und Wissenschaft NRW die Absicherung nach IT-Grundschutz-Methodik des BSI initiiert. Dabei geht es immer darum, die Systeme (insbesondere Netz- sowie Client- und Serversysteme) auf dem neuesten Stand zu halten und Maßnahmen zu implementieren, die eine optimale Ausgewogenheit aus Sicherheit und Bedienbarkeit mit sich bringen. Einer der wichtigsten Faktoren zur Reduzierung der Angriffsvektoren ist und bleibt dabei der Faktor Mensch. Das Ziel der Angreifer ist es, das potenzielle Opfer dazu zu bringen, auf etwas zu klicken und damit ein Stück Software zur Ausführung zu bringen. Dazu setzen sie auf sehr menschliche Komponenten, insbesondere Neugier, Pflichtbewusstsein oder auch Scham. Wie bisher müssen wir auch in Zukunft auf Ihre Hilfe hoffen. Wenn es doch mal passiert ist: seien Sie sich bewusst, dass ein solcher Fehler jedem passieren kann. Schlimmes verhindern können wir nur, wenn Sie das schnellstmöglich weitergeben.

Zurück zur Ursprungsfrage – Alles wieder gut? Nun, in diesem ständigen Auf und Ab der Angreifer und Verteidiger haben wir ein gehöriges Stück aufgeholt und die Hürde für die Angreifer in zentralen Bereichen höher gelegt. Der Vorfall hat dem Thema nicht nur an der RUB hohe Aufmerksamkeit verschafft. Diese ist und bleibt auch notwendig. Bei allen: Anwendern, Administratoren und denjenigen, die an einer Universität die Richtung bestimmen.

HAIKO **TE NEUES**, IT.SERVICES

DIE CLEVERE ALTERNATIVE

Messaging mit Matrix und Element

In der Reihe „Die clevere Alternative“ stellen wir Online-Dienste vor, die an der RUB genutzt werden können und eine Alternative zu gängigen Diensten großer Anbieter darstellen. Über die direkte Anmeldung mit der RUB-LoginID lassen sie sich einfacher in den Alltag der Hochschule einbinden und bieten zudem einen besseren Datenschutz. Die Nutzung für dienstliche Zwecke ist ebenso zulässig.

Matrix ist ein dezentrales Messaging-Protokoll für Desktop und Smartphone, das quelloffen entwickelt wird und Ende-zu-Ende-Verschlüsselung (E2E-Verschlüsselung) unterstützt. Es strebt an, so einfach zu sein wie „WhatsApp“ und so sicher wie „Signal“ und gleichzeitig ein Ersatz für „Slack“ und IRC zu werden.

Matrix erinnert dabei zunächst an E-Mail. Nutzer:innen werden nicht über die Telefonnummer identifiziert, sondern über eine eigene Adresse – an der RUB ist das @<LoginID>:ruhr-uni-bochum.de. Die Nutzung von Matrix an der RUB ist sofort mit Ihrer LoginID möglich. Matrix kann auf verschiedenen Geräten und mit verschiedenen Programmen genutzt werden. Für das Smartphone gibt es die App „Element“, mit der der Dienst genutzt werden kann.

Für den Desktop gibt es die Software „Element“, die ebenfalls als Web-Version verfügbar ist – die App wurde kürzlich von „Riot“ zu „Element“ umbenannt, an der RUB ist der Name „Riot“ noch vielfach synonym in Verwendung.

Es können sowohl öffentliche, themenbezogene Chat-Räume angelegt werden als auch geschlossene, private Chat-Gruppen und direkte 1:1-Chats. Der Chat-Verlauf wird zwischen den verschiedenen von Ihnen genutzten Geräten synchronisiert. Neben Text können auch Bilder gesendet und andere Dateien ausgetauscht werden. Dazu ermöglicht Matrix eine Ende-zu-Ende-Verschlüsselung. Das bedeutet, dass niemand außer den beiden am Chat beteiligten Parteien den Chat lesen kann, auch nicht die Betreiber:innen der Server, wenn diese Verschlüsselung aktiviert ist. Die Nachricht liegt nur am Ende der Empfänger:in und am Ende der Sender:in in im Klartext lesbarer Form vor.

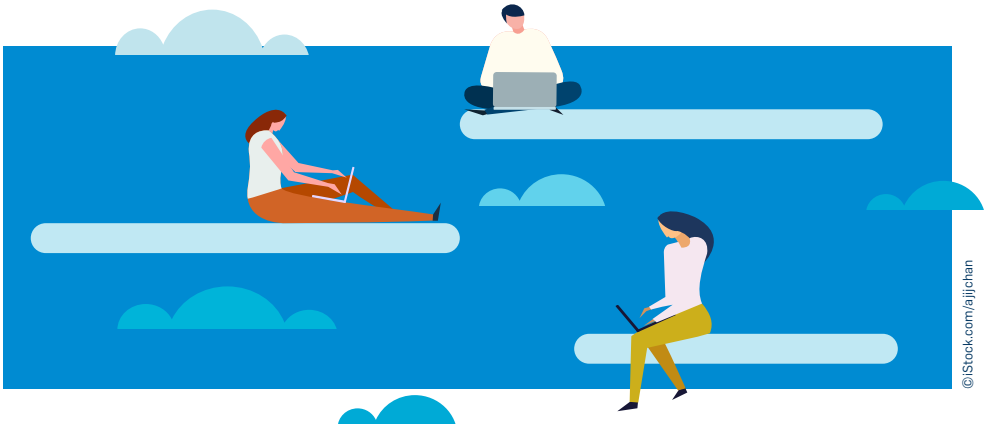
Räume bieten mehr Möglichkeiten zur thematischen Strukturierung und Moderation. So können eigene Räume angelegt werden, die sich für den offenen Austausch zu bestimmten Themen anbieten. Der Raum #Serviceraum-Coronapandemie ist als öffentlicher Raum wie ein Newsletter konfiguriert, in dem wöchentlich alle Änderungen im Zusammenhang mit der Coronapandemie veröffentlicht werden, weitere Nachrichten dort aber nicht möglich sind, sodass insgesamt nur wenige Nachrichten und damit Benachrichtigungen entstehen und der Raum leicht nach Stichwörtern durchsucht werden kann.

Für den Start finden Sie eine Anleitung auf den Seiten von IT.SERVICES. Aktuell findet sich das Angebot an der RUB in einer Erprobungsphase.

CHRISTOPHER **LENTZSCH**, STABSSTELLE DATENSCHUTZ

DIE CLOUD, DER DATENSCHUTZ & **MICROSOFT365**

Die RUB im Schwebezustand



©iStock.com/aijichan

Dass sich Softwarelizenzierung und -nutzung in den vergangenen Jahren stark geändert haben, dürfte mittlerweile fast jeder gemerkt haben. Mit Einschränkungen bei den Nutzergruppen, personenbezogener Lizenzierung und steigenden Kosten optimieren die Anbieter ihre Kontrolle und maximieren die Einnahmen. Eine weitere Baustelle ist die der Cloud: Viele Softwareanbieter verlagern ihre Services in die Cloud, sodass personenbezogene Daten und Datenverarbeitung/-ablage kaum mehr lokal möglich sind.

Neue Lizenzmodelle und digitale Souveränität

Während Unternehmen die neuen Modelle bereits adaptiert haben, tun sich Hochschulen schwer, gerade was die Cloudnutzung angeht. Die Nutzbarkeit von Clouddiensten gemäß DSGVO und den rechtlichen Vorgaben zur Datenverarbeitung/-speicherung sowie das Thema digitale Souveränität (Unabhängigkeit von Global Playern und Hoheit über die Daten) sind Aspekte, die erst langsam in hochschulübergreifenden Gremien diskutiert werden.

Fahrt nimmt die Thematik durch die sehr breite Nutzung von Microsoft-Produkten an den deutschen Hochschulen auf. Mit Start des neuen Bundesvertrages am 1. Mai 2021, an dem auch die Ruhr-Universität Bochum teilnimmt, gilt für Microsoft wie angekündigt die Devise „Cloud first" mit dem Produktportfolio Microsoft365. 2025 soll eine on-premises-Nutzung (d.h. lokaler Server-Betrieb bzw. lokale Installation ohne Microsoft-Account) von Microsoft-Services nach aktuellem Stand gar nicht mehr möglich sein. Durch lizenzrechtliche und technische Vorgaben seitens Microsofts ist aber auch jetzt schon eine reine on-premises-Nutzung sehr stark eingeschränkt.

Zwischen lokaler IT und Cloud

Bedingt durch den neuen Microsoft-Vertrag ergeben sich auch an der RUB etliche Umstellungen bezüglich der Microsoft-Nutzung: Eine personenscharfe Lizenzierung erhöht die Kosten deutlich und technische Umstellungen erfordern die Vergabe von Office365-Lizenzen über die Cloud. Die lokale Installation von Office Professional Plus für Mitarbeiter/innen wird gemäß Vertrag auf eine Lizenz und nur für Computer eingeschränkt. Nur die Aktivierung der Office Apps über die Cloud mit Übertragung von Vornamen, Nachnamen und E-Mail-Adresse ins Azure AD, d.h. Cloud-Verzeichnis von Microsoft, ermöglicht, MS Office mit mehreren Geräten und Geräteklassen nutzen zu können. Die Nutzung von Office 365 für Mitarbeiter/innen und Studierende wird voraussichtlich ab August/September 2021 möglich sein, aktuelle Informationen zum Projekt finden Sie auf der Webseite von IT.SERVICES.

Auf Grund der datenschutzrechtlichen Schwierigkeiten hat das Rektorat sich der mehrheitlichen Meinung der Hochschulen in Deutschland angeschlossen und wird eine Datenverarbeitung in der Cloud und die dortige Speicherung von Daten nicht zulassen können. Services aus Microsoft365 wie Teams, OneDrive, SharePoint Online etc. stehen daher nicht zur Verfügung. Ob und wann Cloud-Applikationen an der RUB freigeschaltet werden können, soll in einem Projekt inklusive hochschulübergreifender Kooperation eruiert werden. Entscheidet man sich, auch vor dem Hintergrund der datenschutzrechtlichen Problematik, gegen eine Nutzung von Microsoft365 in der Cloud, muss jetzt nach Alternativen für etliche Produkte gesucht werden, z.B. SharePoint, Exchange, Office, da diese ab 2025 nach jetzigem Kenntnisstand vielfach nur noch „cloud only" betrieben werden können. Die Hochschulen, die sich bislang beim Thema Cloud-Nutzung eher abwartend verhalten haben, sind nun in Zugzwang, Strategien zum Thema datenschutzkonforme Nutzung und digitale Souveränität zu erarbeiten.

NICOLE **BARGSTEN**, IT.SERVICES

VVT – EINFACH ERKLÄRT

Die seit 2018 geltende Datenschutz-Grundverordnung (DSGVO) sieht zum Nachweis ihrer Einhaltung ein Verzeichnis der Verarbeitungstätigkeiten (VVT) (Art. 30 DSGVO) vor. Dabei handelt es sich um eine spezielle Dokumentationspflicht des Verantwortlichen. In der Praxis ist das VVT der zentrale Bestandteil der Dokumentation. Es kann zwar nicht von jeder Person offen eingesehen werden, doch die zuständige Aufsichtsbehörde kann die Vorlage im Rahmen der behördlichen Kontrolle jederzeit anfragen. Im Rahmen des Pilotprojekts „Umsetzung der DSGVO an der RUB" wurden bereits diverse Dokumente zu den verschiedenen Verarbeitungstätigkeiten der teilnehmenden Organisationseinheiten aus Wissenschaft und Verwaltung erstellt. Nachdem nun erfolgten Abschluss des Projekts und Auswertung der Ergebnisse, soll das VVT jetzt um alle anderen Bereiche der RUB erweitert werden. Ein guter Anlass, um sich die grundlegenden Informationen noch einmal vor Augen zu führen:

Warum ist ein VVT sinnvoll? Neben der gesetzlichen Pflicht, geht es zunächst um die eigene Übersicht, die z.B. hilft, wenn betroffene Personen Auskunftsrechte geltend machen. Weiterhin unterstützt es dabei, die Datenschutzerklärung etwa auf einer Website vollständig zu halten. In diesem Zusammenhang ist die Klarstellung wichtig, dass es sich beim Aufbau des VVT nicht um ein (zeitlich begrenztes) Projekt handelt, sondern um einen fortlaufenden Prozess.

Wer ist verpflichtet und wann muss ein VVT erstellt werden? Grundsätzlich gehören alle Verfahren und Prozesse, bei denen personenbezogene Daten verarbeitet werden, in das Verzeichnis der Verarbeitungstätigkeiten. Personenbezogene Daten sind solche, die sich auf eine natürliche Person beziehen und diese zumindest identifizierbar machen. Verpflichtet sind diejenigen Stellen oder Personen, die über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheiden.

Was passiert, wenn ich kein VVT habe oder es unvollständig ist? Kann die verantwortliche Stelle auf Verlangen der Aufsichtsbehörde kein VVT vorlegen oder ist dies unvollständig, so droht der RUB als öffentliche Stelle zwar nicht direkt ein Bußgeld, jedoch ist zum Beispiel im Rahmen von Schadensersatzprozessen der betroffenen Personen die Wahrscheinlichkeit hoch, dass bei einem Fehlen des VVT zuungunsten der Hochschule von einer mangelhaften Dokumentation auszugehen ist.

Was sind Verarbeitungstätigkeiten und welche gibt es? Eine Verarbeitungstätigkeit ist ein Vorgang, bei dem personenbezogene Daten für einen oder mehrere Zwecke verarbeitet werden. Unter einer Verarbeitung versteht man digitalisierte, aber auch nicht automatisierte Abläufe, bei denen mit personenbezogenen Daten umgegangen wird. Möchte man mit der Eintragung der Verarbeitungstätigkeiten beginnen, kann man sich einen Überblick darüber verschaffen, was im eigenen Bereich bearbeitet wird.

©iStock.com/vulfah

Wo finde ich Beratung und Unterstützung? Das Team des Datenschutzbeauftragten der RUB hilft Ihnen bei Fragen und Problemen gerne weiter.

SABINE **SONNEBORN**, STABSSTELLE SDATENSCHUTZ

NACH EUGH-URTEIL – DATENSCHUTZAUFSICHT PRÜFT **US-TRANSFERS**

©iStock.com/gabort71

Wir berichteten im August letzten Jahres von den rechtlichen Entwicklungen hinsichtlich der Datentransfers in die USA. Der Europäische Gerichtshof (EuGH) hatte im Juli 2020 ein Abkommen zum Datenschutz mit den USA („Privacy Shield") für ungültig erklärt, weitere Anforderungen an andere rechtliche Mechanismen formuliert und die Aufsichtsbehörden zur Durchsetzung gemahnt. Mit weitreichenden Folgen auch an Hochschulen. Die Nutzung vieler (US-) Cloud-Dienste beinhaltet eine entsprechende Datenübertragung. Oft sind auch bei europäischen Alternativen im Hintergrund US-Plattformen im Einsatz. Für die Kooperation mit wissenschaftlichen Partnern in den USA entstehen hier Schranken. In der Praxis sind die Auswirkungen also sehr vielfältig.

Neues Abkommen in weiter Ferne

Die EU-Kommission hatte natürlich unmittelbar begonnen, ein neues Abkommen mit den USA zu verhandeln, das den Anforderungen des EuGH entspricht. Ob ein solches Abkommen zu erreichen ist, bleibt aber sehr fraglich. Die kritisierten Aspekte sind tief im US-amerikanischen Rechtssystem verwurzelt. Dass auf Anfrage von Europäern in den USA Gesetze angepasst werden, ist kaum zu erwarten. In jedem Fall zeichnet sich damit kurzfristig keine Lösung auf diesem Terrain ab.

Neue Standardvertragsklauseln der EU

In Erwartung des EuGH-Urteils hatten bereits vor dessen Entscheidung die meisten Unternehmen sogenannte Standardvertragsklauseln abgeschlossen. Diese ebenfalls von der EU-Kommission beschlossenen Verträge zwischen den beteiligten Unternehmen stammten noch aus 2010. Damals begannen die ersten Überlegungen zur Datenschutzgrundverordnung. Eine Aktualisierung erhielt nun also höhere Priorität und in der Tat liegen seit 4. Juni nun die neuen Versionen der Verträge vor. Falls die alten Verträge noch Bestandteil einer Kooperation sind, besteht nun eine Übergangsfrist von eineinhalb Jahren, um auf die neuen Verträge umzustellen.

„Handlungsleitfaden"

Aufgrund der rechtlich unsicheren Situation haben die Aufsichtsbehörden für den Datenschutz weitere Klärung angestrebt. Ziel ist es dabei, eine einheitliche Rechtsauslegung zu finden. Der europäische Datenschutzausschuss (EDSA), ein Gremium, in dem die Aufsichtsbehörden der Mitgliedsstaaten Konsistenz herstellen müssen, hatte seither an „Praxisleitfäden" gearbeitet. Ein noch nicht abschließend veröffentlichter, aber abgestimmter Entwurf der Maßnahmen, die die Standardvertragsklauseln ergänzen, liegt seit November 2020 vor. Im Wesentlichen wird ein allgemeiner Prozess zur Beurteilung von Drittstaatentransfers beschrieben. Dieser dürfte nur in seltenen Fällen für die US-Transfers eine gangbare Lösung ermöglichen. Beispielsweise kann man weitgehend pseudonymisierte Forschungsdaten im Ergebnis übertragen. Der Analyseprozess dahin darf aber als aufwendig bezeichnet werden. Die eigentliche Idee des EU-Gesetzgebers (DSGVO), durch Kommissionsentscheidungen den freien Datenverkehr zu vereinfachen, ist hier weitgehend konterkariert. Der offizielle Beschluss des sicher nur geringfügig geänderten Entwurfs des Handlungsleitfadens dürfte nicht mehr in weiter Ferne liegen. Damit werden die Anforderungen belastbarer, entsprechende Handlungen damit dringlicher. Nicht alle offenen Fragen sind hier aber abschließend beantwortet und einige Themen bleiben unklar. So ist rechtlich beispielsweise offen, ob eine vertraglich festgelegte Verarbeitung bei einem US-Dienstleister in einem europäischen Rechenzentrum den Anforderungen genügt. Die Aufsichtsbehörden und Gerichte scheinen hier uneinig.

Durchsetzung durch die Aufsichtsbehörden

Der EuGH hatte in seinem Urteil die Datenschutzaufsicht zur Rechtsdurchsetzung gemahnt. Der Finger zeigte dabei nicht nur nach Irland – der eigentliche Auslöser des Falls war ein Rechtsstreit mit Facebook im Zuständigkeitsbereich der irischen Aufsicht – sondern auch auf die anderen Aufsichtsbehörden. In Europa werden erste Untersagungen von US-Datentransfers bekannt. Nach einem Jahr war demnach nun genug Zeit für eine Umstellung. Bei den deutschen Aufsichtsbehörden ist die Spannbreite noch recht groß: einige haben bereits klare Aussagen zu einzelnen Systemen getroffen, andere halten sich hier noch zurück. Kürzlich haben sich aber mehrere Aufsichtsbehörden in Deutschland zu einer Fragebogenaktion entschlossen, bei der Unternehmen offenlegen sollen, wie sie seither handeln. Das muss als erster Schritt verstanden werden. KUL

HERAUSGEBER Dr. Kai-Uwe Loser (v.i.S.d.P.), KUL, Behördlicher Datenschutzbeauftragter der RUB (bDSB); Brigitte Wojcieszynski (v.i.S.d.P.), BW, Beauftragte für Informationssicherheit der RUB (ITSB); Birgit Steiner, BS, stellv. Beauftragte für Informationssicherheit der RUB (ITSB); Anschrift: Ruhr-Universität Bochum, Geschäftszimmer Stabsstelle Informationssicherheit, GAFO 04/622, Kerstin Bussmann, 44780 Bochum, Telefon: 0234/32-24888, E-Mail: rubinform@rub.de; Infos: www.rub.de/rubinform; Titelbild: ©Hans Blossey

WEITERE INFOS

ZU UNSEREN THEMEN IM NEWSLETTER:

CYBERANGRIFF AUF DIE RUB – ALLES WIEDER GUT?

Rückblick auf 2020 – Der Jahresbericht von IT.SERVICES:
https://www.it-services.ruhr-uni-bochum.de/mam/content/pdf/jahresbericht_2020_online.pdf

DIE CLEVERE ALTERNATIVE: MESSAGING MIT **MATRIX UND ELEMENT**

Infos und Anleitung zum Messenger Element*: https://www.it-services.ruhr-uni-bochum.de/services/issi/element.html.de*

DIE CLOUD, DER DATENSCHUTZ & **MICROSOFT365**

Microsoft-Nutzung an der RUB: *https://it-services.ruhr-uni-bochum.de/services/software/microsoft.html.de*

VVT – EINFACH ERKLÄRT

Das Team des Datenschutzbeauftragten an der RUB: *https://dsb.ruhr-uni-bochum.de/*

DATENSCHUTZAUFSICHT PRÜFT **US-TRANSFERS**

Presseerklärung zur Verhandlung eines neuen Abkommens zum Datenschutz
https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443

Neue Standardvertragsklauseln für Datentransfer zwischen EU und Nicht-EU-Staaten:
https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

Entwurf von Maßnahmen/Praxisleitfäden:
https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_en

Koordinierte Prüfung internationaler Datentransfer mit Link zum Fragebogen:
https://datenschutz-hamburg.de/pressemitteilungen/2021/06/2021-06-01-fragebogen-datentransfer