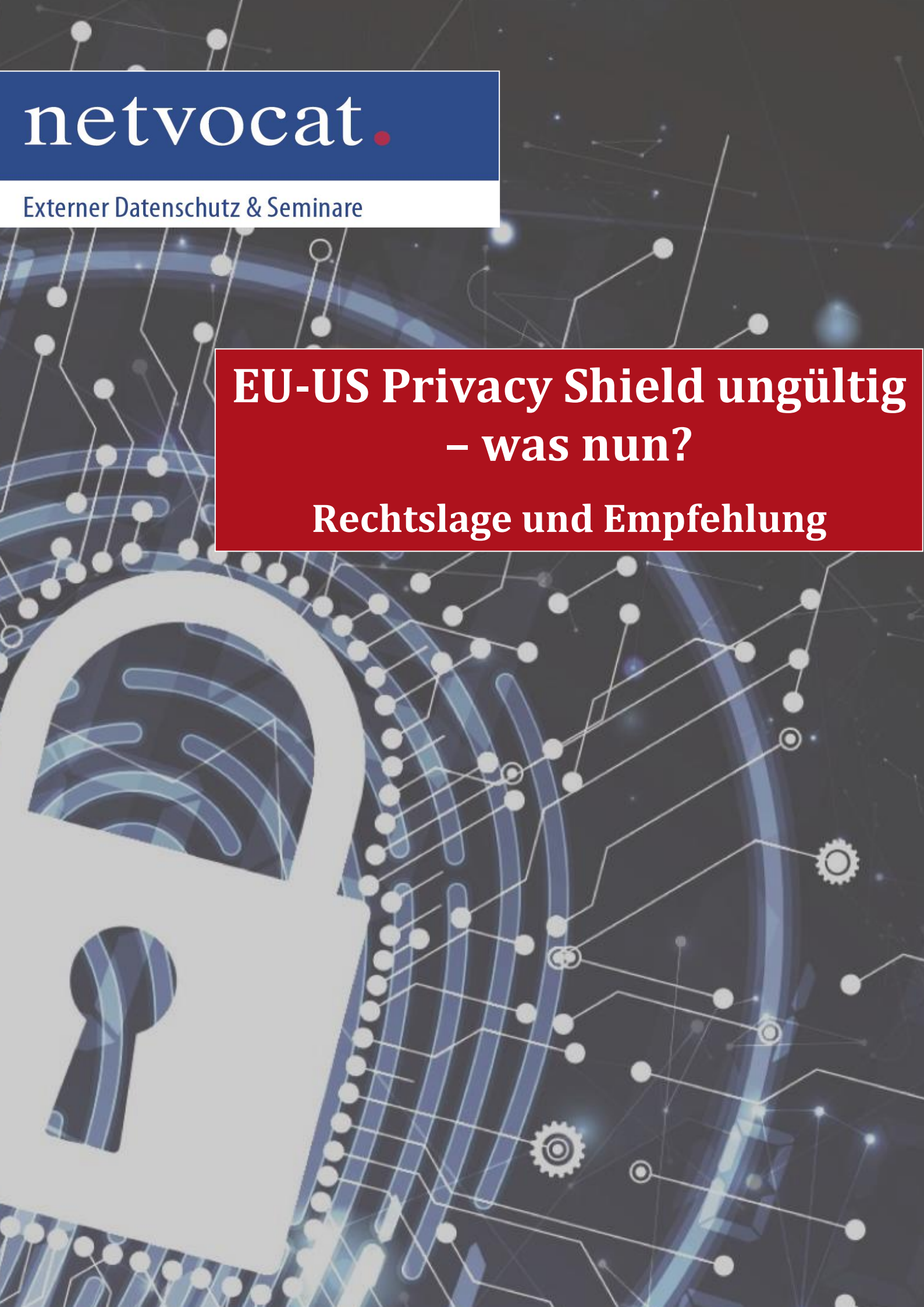
netvocat.

Externer Datenschutz & Seminare

EU-US Privacy Shield ungültig – was nun?

Rechtslage und Empfehlung



Inhalt

Über uns

Sie benötigen Unterstützung und Beratung im Bereich des Datenschutzes? Dann sind Sie bei uns richtig!

Wir sind spezialisiert im Bereich der Datenschutzberatung und bieten in diesem Bereich sowohl sämtliche Dienstleistungen eines externen Datenschutzbeauftragten, als auch die Betreuung und Beratung im Hinblick auf einzelne datenschutzrechtliche Projekte oder Fragen an.

Zu unseren Mandanten zählen Unternehmen jeglicher Größe (internationaler Konzern bis Einzelunternehmer), die in unterschiedlichen Branchen tätig sind (IT, Groß- und Einzelhandel, Marketing und Werbung, Ingenieurwesen, Gesundheitswesen etc.). Darüber hinaus sind wir auch für öffentliche Institutionen tätig.

Überlassen Sie uns den Datenschutz – damit Sie Zeit für Ihr Unternehmen haben.

Als externe Datenschutzbeauftragte versuchen wir, sämtliche datenschutzrelevanten Abläufe in Ihrem Unternehmen schnellstmöglich rechtskonform zu gestalten. Hierzu prüfen wir zunächst den Stand Ihres Unternehmens in Bezug auf Datenschutz und erarbeiten sodann einen Maßnahmenplan, den wir gemeinsam mit Ihnen umsetzen. Die Tätigkeit als externe Datenschutzbeauftragte ist grundsätzlich auf eine langfristige vertrauensvolle Zusammenarbeit angelegt.
Unsere Beratungsleistungen im Projektbereich können jederzeit kurzfristig und ohne Vertragsbindung beauftragt werden.
Bei sämtlichen Aufgaben ist uns wichtig, dass wir Ihnen unsere Maßnahmen verständlich machen und Ihre wirtschaftlichen Interessen bei der Umsetzung berücksichtigen.

Aus aktuellem Anlass möchten wir Sie heute nachfolgend über wichtige Neuigkeiten im Datenschutzrecht informieren.

Mit freundlichen Grüßen
Daniela Wagner-Schneider, LL.M.
Geschäftsführerin | Rechtsanwältin | Datenschutzbeauftragte DSB TÜV
netvocat® GmbH – Externer Datenschutz & Seminare

Das Urteil des EuGH

Der EuGH hat in seinem gestern verkündeten Urteil (16. Juli 2020, Az.: C-311/18) in dem Vorabentscheidungsverfahren, das durch den irischen High Court ersucht worden war und die Beschwerde des österreichischen Bürger Schrems zur Grundlage hat, den Beschluss der Kommission (EU) 2016/1250 über die Angemessenheit des vom EU-US-Datenschutzschild („Privacy Shield“) gebotenen Datenschutzes für ungültig erklärt. Dies bedeutet, dass der Transfer personenbezogener Daten von der EU an US-Unternehmen rechtswidrig ist, da die Rechtsgrundlage des Privacy Shield mit diesem Urteil sofort entfällt. Der EuGH hat auch festgestellt, dass es keine Übergangsfrist gibt.

Der EuGH begründet seine Entscheidung damit, dass trotz des Privacy Shield US Behörden berechtigt waren, auf Daten von EU Bürgern zuzugreifen und es für EU Bürger hiergegen keine Rechtsmittel gab - z. B. erlaubt Section 702 des Foreign Intelligence Surveillance Act (FISA) Datenzugriffe auf Daten von Nicht-US-Bürgern in elektronischen Kommunikationsmitteln wie E-Mails ohne gerichtlichen Beschluss.

Die Pressemitteilung Nr. 91/20 finden Sie hier:
https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091de.pdf

Das Urteil des EuGH finden Sie hier:
http://curia.europa.eu/juris/document/document.jsf?docid=228677&mode=lst&pageIndex=1&dir=&occ=first&part=1&text=&doclang=DE&cid=9819512

Bisherige Rechtslage

Grundsätzlich ist nach der DSGVO ein Transfer personenbezogener Daten in sog. „Drittländer“ verboten, wenn diese Länder gem. Art. 44-49 DSGVO kein angemessenes Datenschutzniveau vorweisen können. Zu diesen Ländern gehören u. a. auch die USA.
Daher musste man bei einem Transfer in solche Länder zunächst prüfen, ob ein angemessenes Datenschutzniveau gegeben ist.
In folgenden Fällen wurde ein angemessenes Datenschutzniveau unterstellt und somit Datentransfers in Drittländer als zulässig erachtet:

- Aufgrund eines **Angemessenheitsbeschlusses** der EU-Kommission, d. h. die Kommission hat per Beschluss das Datenschutzniveau für ein Land festgestellt.
- Abschluss von **Standardvertragsklauseln** (standard contractual clauses (SCC)), d. h. es wurde zwischen den Vertragspartnern (Datenexporteur und Empfänger) dieser von der EU vorgegebene Mustervertrag geschlossen, der regelt, dass der Datenempfänger (Unternehmen im Drittland) sich den Regeln des Datenschutzes in der EU unterwirft und dies auch tatsächlich geschieht, was geprüft werden muss.
- Transfer an Unternehmen, die sog. **Binding Corporate Rules** (BCR) besitzen, ein Regelkatalog mit strengen Datenschutzregeln, der von einer Datenschutzbehörde zertifiziert werden muss.
- Aufgrund der **Erforderlichkeit der Datenübertragung** oder einer erforderlichen Datenverarbeitung in einem Drittland, sofern dies für die Betroffenen erkennbar ist, z. B. wenn bei Buchung einer Reise in die USA personenbezogene Daten der Reiseteilnehmer zur Abwicklung der Buchung/Reise dorthin versendet werden.
- Aufgrund von **Einwilligungen der Betroffenen** in den Datentransfer oder –bearbeitung im Drittland, die jedoch jederzeit widerrufen werden kann und in einigen Fällen auch unzulässig sein kann.
- Aufgrund des **EU-US Privacy Shield**, das als Abkommen zwischen den USA und der EU-Kommission das Datenschutzniveau durch verbindliche Verpflichtung der USA zur Einhaltung des Datenschutzes nach EU-Maßstab regelte.
- Aufgrund weiterer **Ausnahmen gem. Art. 49 DSGVO**.

Aktuelle Rechtslage

In der Vergangenheit stützte man sich daher als Rechtsgrundlage für Datentransfers in die USA auf das EU-US Privacy Shield.

Durch das Urteil des EuGH fällt diese Rechtsgrundlage nun weg mit der Folge, dass Datentransfers in die USA, die sich ausschließlich auf das Privacy Shield gestützt hatten, nun rechtswidrig sind. Da es auch keine Übergangsfrist gibt, gilt dies unmittelbar.

Standardvertragsklauseln = Lösung?

Der EuGH hat in seinem heutigen Urteil auch zu den Standardvertragsklauseln Stellung genommen und entschieden, dass der Beschluss der Kommission 2010/87 über die Standardvertragsklauseln gültig ist.

Dies bedeutet, dass Datentransfers in die USA grundsätzlich auf Standardvertragsklauseln als Rechtsgrundlage gestützt werden können.

ABER: Nach Auffassung des EuGH ist zu beachten, dass „*nach dem Beschluss der Kommission der Datenexporteur und der Empfänger der Übermittlung vorab prüfen müssen, ob das erforderliche Schutzniveau im betreffenden Drittland eingehalten wird, und dass der Empfänger dem Datenexporteur gegebenenfalls mitteilen muss, dass er die Standardschutzklauseln nicht einhalten kann, woraufhin der Exporteur die Datenübermittlung aussetzen und/oder vom Vertrag mit dem Empfänger zurücktreten muss*“ (Pressemitteilung Nr. 91/20).

De Facto bedeutet dass, dass vor Abschluss der Standardvertragsklauseln tatsächlich geprüft und festgestellt werden muss, ob in dem Drittland ein angemessenes Datenschutzniveau herrscht.

In Bezug auf die USA hat der EuGH heute jedoch entschieden, dass in den USA kein angemessenes Datenschutzniveau gegeben ist, so dass Datentransfers in die USA auch nicht mehr aufgrund der Standardvertragsklauseln rechtmäßig sein können.

Welche Datentransfers sind betroffen?

Betroffen sind grundsätzlich nur Transfers von personenbezogenen Daten. Darunter fallen nicht reine Unternehmens- oder anonymisierte oder sonstige Maschinendaten.

Unter Datentransfers in die USA fasst man nicht nur den Versand von personenbezogenen Daten per elektronische Kommunikationsmittel wie E-Mails.

Darunter fallen auch der Einsatz von Tools und Cookies von US Anbietern auf eigenen Webseiten, in Apps etc., da hier personenbezogene Daten wie IP-Adressen auf Server in die USA transferiert werden.

Auch die Inanspruchnahme von Diensten, die von US Unternehmen angeboten und betrieben werden und die die erhobenen Daten auf US Servern speichern und verarbeiten, fällt darunter.

Beispiele:

- Analysetools wie Google Analytics
- Newsletteranbieter wie Mailchimp
- Plugins und Fanpages von sozialen Netzwerken wie Facebook
- Anwendungen wie Google Maps
- Cloud Anbieter wie Microsoft

Welches Risiko besteht?

Jegliche Transfers personenbezogener Daten in die USA sind seit gestern rechtswidrig.

Abmahnungen von Betroffenen

Nach der DSGVO können auch Betroffene die Unternehmen abmahnen und Schadenersatz verlangen. Sie können also verlangen, dass ihre Daten nicht mehr in die USA gesendet werden und die Dienstleistung einzustellen ist.

Abmahnungen von Mitbewerbern

Diese Abmahnungen werden sich in erster Linie auf die nunmehr falschen Angaben in den Datenschutzerklärungen und Cookie Bannern beziehen. Allerdings ist aktuell noch vom EuGH zu klären, ob Abmahnungen wegen Datenschutzverstößen aufgrund Wettbewerbsrechts überhaupt zulässig sind.

Anordnungen der Behörden

Die Datenschutzaufsichtsbehörden werden nun auch aktiv werden und ggfs. Kontrollen in Unternehmen durchführen oder Anfragen senden. Im schlimmsten Fall werden die Datentransfers untersagt und ein Bußgeld angedroht (bis zu 4 % des Umsatzes).

Was ist zu tun?

Es bleibt nun die Frage, wie man aufgrund des Urteils agieren soll und welche rechtliche Lösung es zeitnah geben kann. Die Antwort ist: Es wird zeitnah keine geben. Dazu ist die Entscheidung zu neu. Es müssen sich nun erst einmal Behörden, DSK und andere Institutionen zum Urteil äußern und Lösungsansätze entwickeln.

Nichtsdestotrotz müssen Unternehmen zeitnah handeln, da die Rechtswidrigkeit der Datentransfers in die USA seit gestern feststeht.

Angesichts dessen empfehlen wir aktuell folgende Maßnahmen, bei denen wir Sie unterstützen werden:

- Klären Sie schnellstmöglich, **welche personenbezogenen Daten** von Ihrem Unternehmen in die USA, z. B. wegen Anwendung der o. g. Tools oder Dienste oder durch sonstige Transfers, gesendet werden. Hierzu müssen Sie zunächst herausfinden, welche Tools und Dienste Sie einsetzen und ob diese von US Anbietern betrieben werden.

- Fragen Sie die Anbieter aktiv oder finden Sie heraus, ob die Daten auf US Servern verarbeitet werden oder **ob die Anbieter auch EU Server betreiben** und die Möglichkeit besteht, die Daten nur dort zu verarbeiten (z. B. möglich bei Amazon Web Services oder Microsoft).

- Falls Sie keine oder unzureichende Antworten erhalten, **wechseln Sie – wenn möglich – umgehend zu EU Anbietern**, die ihre Server tatsächlich in der EU betreiben.

- Oder **wechseln Sie zu US Anbietern, die neben Servern in den USA auch Server in Europa betreiben** und tatsächlich gewährleisten (können), dass die Daten nur auf EU Servern verarbeitet werden.

- Setzen Sie **keine Tools oder Dienste von Anbietern (mehr) ein, die mit Subunternehmern in den USA arbeiten** und die Daten daher in den USA verarbeiten.

- Wenn kein Wechsel möglich ist, müssen Sie den Anbieter zum **Abschluss von Standardvertragsklauseln** auffordern. Der EuGH hat sich zwar kritisch zur Wirksamkeit geäußert und setzt eine strenge Prüfung des Datenschutzniveaus voraus, was faktisch in den USA nicht bejaht werden kann. Dennoch hat der EuGH diese Verträge nach wie vor für gültig erklärt, weshalb unbedingt auf diese zurückgegriffen werden sollte.

- Wenn der Abschluss von Standardvertragsklauseln nicht möglich ist, sollten **Einwilligungen der Betroffenen** eingeholt werden, auch wenn dies eine auf lange Sicht unsichere Rechtsgrundlage ist.

- Die **Datenschutzerklärungen sind anzupassen**, da für sämtliche Tools das Privacy Shield nicht mehr als Rechtsgrundlage benannt werden darf. Diese Angabe muss daher entfernt werden.

- Dienstleister, die selbst für die Verarbeitung der Daten (z. B. die Daten ihrer Kunden) verantwortlich sind, sollen ihre **technisch-organisatorischen Maßnahmen gem. Art. 32 DSGVO anpassen** und eventuell veränderte Datenschutzeinstellungen gem. Art. 25 DSGVO implementieren.

- **Dokumentieren Sie** Ihre o. g. Bemühungen, falls seitens der Aufsichtsbehörden nachgefragt wird, was Sie unternommen haben.

- Verfallen Sie nicht in Panik. Viele denken jetzt zwar wieder, dass sofort alle Fanpages auf sozialen Netzwerken gelöscht werden müssen. Und ja, es gibt jetzt das Risiko von Abmahnungen und behördlichen Untersagungen. Dennoch muss man abwägen, ob man seine hart erkämpften Follower ziehen lassen will oder auf eine Lösung der Netzwerke wie Facebook & Co. warten möchte, die sicher bald Serverlösungen in der EU anbieten werden.

Wir weisen nochmals darauf hin, dass die Datenschutzerklärungen und Cookie Banner schnellstmöglich anzupassen sind (s. o.). Gerne übernehmen wir das für Sie.

Kontakt

netvocat® GmbH – Externer Datenschutz & Seminare
Großherzog-Friedrich-Str. 40
66111 Saarbrücken
Tel.: 0681/590 97 98 – 50
Fax: 0681/590 97 98 – 30
E-Mail: info@netvocat.de
Internet: www.netvocat.de

Öffnungszeiten:

Sie erreichen uns von Montag bis Freitag von 09:00 Uhr bis 17.00 Uhr.

Aktuell erreichen Sie uns am besten per **E-Mail oder Telefon** unter den o. g. Adressen und Nummern.
Gerne bieten wir auf Nachfrage auch **Web-Meetings** an.

Weitere Ansprechpartner:

Ihre Ansprechpartner für neue Anfragen sind:

- Daniela Wagner-Schneider, LL.M., Geschäftsführerin, Rechtsanwältin, Datenschutzbeauftragte DSB TÜV: dwagner-schneider@netvocat.de

- Elina König, Diplom-Juristin, Datenschutzbeauftragte DSB TÜV: eko-enig@netvocat.de

Wir sind gerne für Sie da – sprechen Sie uns an!

Impressum:

1. Auflage

Herausgeber:
netvocat GmbH – Externer Datenschutz & Seminare
Großherzog-Friedrich-Str. 40
66111 Saarbrücken
Tel.: 0681/590 97 98 – 50
Fax: 0681/590 97 98 – 30
E-Mail: info@netvocat.de
Internet: www.netvocat.de

Grafik: © kras99/stock.adobe.com