Ausgabe 2 | Dezember 2019

Wir wünschen Ihnen frohe Weihnachten
und ein erfolgreiches Jahr 2020.

Inhalt:

In der Weihnachts-bäckerei …

Alexander Hausner

… gibt es neben Keksen, auch Cookies genannt, auch andere Leckereien. Wie Rolf Zuckowski in seinem Weihnachtsevergreen könnten auch wir in Bezug auf die Anwendung der DSGVO oft beklagen, dass das Rezept versteckt wurde und wir nun frei nach Schnauze backen müssen. Aber hinter manchen Tannenwipfeln ungeklärter Fragen kann man schon bunte Lichtlein der Erkenntnis blitzen sehen. Auch wenn einem diese Lichtlein manchmal nicht gefallen dürften.

So wurde zunächst im September von der Deutschen Datenschutzkonferenz DSK verkündet, dass sich die deutschen Datenschutzbehörden im Juni 2019 auf ein **einheitliches Konzept zur Berechnung von Bußgeldern** nach Art. 83 DSGVO verständigt haben. Das Modell soll auf Basis des Umsatzes des verantwortlichen Unternehmens nach Art und Schwere des datenschutzrechtlichen Verstoßes, seiner Auswirkungen auf betroffene Personen sowie nach dem Verschuldensgrad des Verantwortlichen und den Gesamtumständen eine objektivierbare, gerechte Bußgeldzumessung ermöglichen und Bußgelder vermeiden, die außer Verhältnis zur Tat stehen.

Wohl in Anwendung dieses Bußgeldberechnungskonzeptes verhängte die Berliner Aufsichtsbehörde dann am 5. November 2019 das **bisher höchste deutsche Bußgeld in Höhe von 14,5 Millionen Euro** gegen den Immobilienkonzern „Deutsche Wohnen SE“. Soweit bekannt, wurden personen-bezogene Daten archiviert, wobei der Grund hierfür von der Aufsichtsbehörde nicht als ausreichend angesehen wurde. Gegebenenfalls kollidieren hier die Interessen an einer revisionssicheren Speicherung aus steuerlichen Gründen mit datenschutzrechtlichen Sparsamkeitsvorstellungen. Das wird sich wohl in einem kommenden Gerichtsverfahren aufklären. Aus den Aufsichtsbehörden ist jedenfalls zu vernehmen, dass in Zukunft vermehrt mit höheren Bußgeldern zu rechnen sein wird. Morgen, Kinder, wird‘s was geben …

Unter dem 8. Oktober 2019 wurde vom Europäischen Datenschutzausschuss (EDSA) die finale „Leitlinie 2/2019 zur Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 lit. b DSGVO im Rahmen der Bereitstellung von Online-Diensten für betroffene Personen“ veröffentlicht. Der EDSA konkretisiert in dieser **Leitlinie** die Anforderungen an die **„Erforderlichkeit“ einer Datenverarbeitung** für die Durchführung eines Vertrages. Was nach einer sinnvollen Maßnahme klingt, um Unklarheiten in der Auslegung der DSGVO zu minimieren, entpuppt sich bei näherer Betrachtung leider weniger als ein Öffnen der Lebkuchendose als eines der Büchse der Pandora. Nach Auffassung der EDSA (in Fortführung der Ansichten der Artikel-29-Gruppe) ist die „Erforderlichkeit“ bei Art. 6 Abs. 1 lit. b DSGVO eng auszulegen, die **Datenverarbeitung muss wirklich notwendig** („genuinely and objectively necessary“) **für die Vertragsdurchführung** sein. Abzustellen ist für den verantwortlichen Unternehmer also auf den konkreten Vertrag, nicht auf seinen Geschäftszweck. Damit können zusätzliche Datenverarbeitungen für Marketingzwecke oder Geschäftsoptimierungen nicht auf Art. 6 Abs. 1 lit. b DSGVO gestützt werden. Eine Vertragsgestaltung hierzu, bisher oft auch durch AGBs, ist damit mehr als risikobehaftet. Eine weiter gefasste Auslegung einer Erforderlichkeit einer Datenverarbeitung schließt die EDSA dann für den Anwendungsbereich des Art. 6 Abs. 1 lit f DSGVO zwar nicht aus. Hier wird sich aber zeigen, ob und inwieweit in der Praxis tatsächlich eine offene Interessensabwägung nach lit. f zugelassen werden wird, obwohl eine Regelung dazu im konkreten Vertrag nicht als Rechtfertigung für die Datenverarbeitung ausgereicht hätte. Denn auch schon bisher konnte neben lit. b der Rechtfertigungsgrund nach lit. f nur dann zur Anwendung kommen, wenn vertragliche Schutzpflichten nicht verletzt werden. Da dann aber weder aus dem Vertrag noch aus der gesamten Geschäftsbeziehung heraus etwa eine Webanalyse durchgeführt werden dürfte, sollte dem Weihnachtsmann auf die Wunschliste geschrieben werden, dass es doch auch im europäischen Primärrecht ein Recht auf Unternehmensfreiheit gibt. Es droht sonst ein höchst unchristlicher **Kreuzzug** des **Datenschutzes** gegen die **digitale Marktwirtschaft**.

Am 14. November 2019 veröffentlichten die Datenschutzaufsichtsbehörden der Länder dann abgestimmte Pressemitteilungen, in denen mitgeteilt wurde, dass Website-Betreiber **Einwilligungen** der Website-Besuchenden benötigen, wenn sie **Drittdienste** einbinden wollen, bei denen dieser Drittanbieter personenbezogene Daten der Besuchenden

auch für eigene Zwecke nutzt. Dazu gehört jedenfalls auch das im Markt beliebte Produkt Google Analytics. Zu beachten ist, dass die Pflicht zur Einholung einer aktiven Einwilligung dabei **nicht auf** die Einbindung von Drittdiensten mithilfe von **Cookies beschränkt** ist. Der Verantwortliche kann sich nach Ansicht der Aufsichtsbehörden also etwa für den Einsatz von Analysetools von Drittanbietern mit Eigeninteressen nicht mehr auf ein nicht überwiegendes Interesse der betroffenen Personen i. S. d. Art. 6 Abs. 1 lit. f DSGVO berufen. Eigene Analysetools ohne Weitergabe von Daten an Dritte sind davon aber nicht betroffen. Die selbst gehostete Webanalyse wird dann also nur an der oben beschriebenen Erforderlichkeit für die Vertragsdurchführung zu messen sein.

Sowohl die Leitlinie 2/19 der EDSA als auch die Anforderungen an Einwilligungen bei der Einbindung von Drittdiensten macht das Bemühen deutlich, die Grundsätze der Transparenz der Datenverarbeitung und der Datenminimierung durchzusetzen. Die von der Datenverarbeitung betroffenen Personen sollen davor geschützt werden, dass ihre Daten von einem Verantwortlichen genutzt werden, ohne dass dies offensichtlich erkennbar ist. Bei der konkreten Vertragsdurchführung ergibt sich die Offensichtlichkeit für die betroffene Person aus dem direkten Leistungsaustausch. Bei der Einbeziehung anderer Zwecke oder gar dritter Parteien muss also nicht nur aufgeklärt, sondern wohl auch eine Einwilligung eingeholt werden. Die betroffene Person soll auf Augenhöhe mit dem Verantwortlichen über die Verwendungsmöglichkeiten ihrer Daten verhandeln können; Transparenz als Mittel zur Fairness.

Nun aber kann sie kommen, die Stille Nacht. Die wird übrigens stiller als sonst, denn wir werden vielleicht singen müssen: „Alle Jahre wieder, kommt das [ausgeblendet nun ein Artikel 9 DSGVO Datum zu einem Kind]“.

Alexander Hausner LL. M.

Rechtsanwalt, Fachanwalt für Arbeitsrecht, zert. Datenschutzbeauftragter

Telefon: +49 40 4223 6660-0
E-Mail: a.hausner@roser-hamburg.de

Weihnachtsgrüße und Datenschutz

Jessica Stehn-Bäcker

Weihnachten ist die Zeit der Besinnlichkeit. Man blickt auf das vergangene Jahr zurück und möchte sich vielleicht bei der ein oder anderen Person für die gute Zusammenarbeit bedanken und alles Gute für das kommende Jahr wünschen.

Doch geht das eigentlich noch zu Zeiten der Datenschutzgrundverordnung (DSGVO) – Weihnachtskarten versenden?

Vorüberlegung

Die DSGVO regelt den Umgang oder genauer gesagt die Verarbeitung von personenbezogenen Daten (Name, postalische Anschrift, Geburtsdatum etc.) einer natürlichen Person.

Es gelten hierbei sechs Grundsätze für die Datenverarbeitung:

1. Sie muss auf rechtmäßige Weise, nach Treu und Glauben sowie transparent erfolgen.
2. Sie darf nur für festgelegte, eindeutige und legitime Zwecke genutzt werden.
3. Sie muss dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Datensparsamkeit).
4. Sie muss dem Prinzip der Richtigkeit folgen.
5. Daten dürfen nur über einen begrenzten Zeitraum gespeichert werden.
6. Das Prinzip der Integrität und Vertraulichkeit muss eingehalten werden.

Bei jeder Verarbeitung von personenbezogenen Daten muss sich der Verantwortliche an die datenschutzrechtlichen Bestimmungen der DSGVO und an diese sechs Grundsätze halten. Folglich auch beim Versand von Weihnachtsgrüßen.

Rechtsgrundlage: Weihnachtskarte per Post

Der Versand von Weihnachtskarten ist eine Verarbeitungstätigkeit und benötigt folglich eine Rechtsgrundlage nach Art. 6 DSGVO.

Zunächst kommt die Einwilligung des Empfängers nach Art. 6 Abs. 1 lit. a DSGVO in Betracht. Diese im Vorwege beim Empfänger einer Weihnachtskarte einzuholen ist eine eher unrealistische Aufgabe, die allerdings auch nicht notwendig ist. Denn die Kontaktpflege zu Bestandskunden, Kooperationspartnern usw. fällt unter Art. 6 Abs. 1 lit. f DSGVO, dem berechtigten Interesse.

Dieser Erlaubnistatbestand legitimiert eine Verarbeitungstätigkeit, wenn diese zur Wahrung berechtigter Interessen erforderlich ist und unter anderem die Interessen der betroffenen Person nicht überwiegen. Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung, folglich auch für einen Weihnachtsgruß, kann insoweit als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden. Zudem kann ein berechtigtes Interesse auch dann vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht (zum Beispiel wenn die betroffene Person ein Kunde des Verantwortlichen ist).

Sofern sich der Verantwortliche also mit seiner Weihnachtskarte für die Zusammenarbeit im vergangenen Jahr bedanken möchte, so kann er sich auf das berechtigte Interesse nach Art. 6 Abs. 1 lit. f DSGVO stützen.

Rechtsgrundlage: Weihnachtsgrüße per E-Mail

Beim Versand einer weihnachtlichen Grußbotschaft per Mail gestaltet sich es allerdings anders: Der Empfänger muss vorab seine Einwilligung zum Erhalt von Werbenachrichten gegeben haben. Denn ein Weihnachtsgruß per Mail gilt ja als Werbemaßnahme.

Eine Ausnahme gibt es allerdings: Sofern ein Unternehmen im Zusammenhang mit dem Verkauf einer Ware oder der Erbringung einer Dienstleistung die E-Mail-Adresse des Kunden erhalten hat, darf er diese zur Direktwerbung – und folglich auch für den Versand eines weihnachtlichen Grußes – verwenden.

Informationspflichten

Auch beim Versand von Weihnachtskarten sind die Informationspflichten nach Art. 12 ff. DSGVO zu erfüllen. Hat der Verantwortliche den Empfänger bislang noch nicht über den (allgemeinen) Umgang mit personenbezogenen Daten informiert, so ist es an der Zeit, dies nachzuholen. Denn nur wer weiß, dass über ihn Daten verarbeitet werden und welche Rechte er hierbei hat, kann diese Rechte auch in Anspruch nehmen.

Nachfolgende Angaben sind dabei regelmäßig zu machen:

- Name und Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten (sofern benannt)
- Zwecke, für die die personenbezogenen Daten erhoben und verarbeitet werden
- Rechtsgrundlage
- Dauer der Speicherung
- Empfänger oder Kategorien von Empfängern
- Verarbeitungsort/Speicherort
- das Bestehen der Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch und Datenübertragbarkeit
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde für Datenschutz
- ggf. das Bestehen eines Rechts, die Einwilligung jederzeit für die Zukunft zu widerrufen

Aber wie kann man dem Empfänger der Weihnachtsbotschaft diesen Informationstext ohne Aufwand zur Kenntnis geben? Auch hier empfiehlt sich die sogenannte Link-Lösung: Der Text wird auf der unternehmenseigenen Internetseite unter einer eingängigen Adresse (www.musterfirma.de/datenschutzhinweise) veröffentlicht und dieser Link auf der Weihnachtskarte abgedruckt bzw. in der E-Mail aufgenommen.

Verarbeitungsverzeichnis

Der Verantwortliche ist nach Art. 30 Abs. 1 DSGVO dazu verpflichtet, über seine Verarbeitungstätigkeiten von personenbezogenen Daten ein Verzeichnis zu führen. Auch der Versand von Weihnachtspost sollte hier aufgenommen werden.

Praxistipp

Bevor die Weihnachtsgrüße auf Reisen gehen, ist eine Bestandsaufnahme sinnvoll.

Erstellen Sie eine Liste aller geplanten Empfänger und prüfen Sie diese nach oben genannten Kriterien: Möchten Sie sich beim Empfänger für die gute Zusammenarbeit im letzten Jahr bedanken? Ist der Empfänger im letzten Jahr noch Kunde/Dienstleister etc. gewesen? Hat der Empfänger dem Erhalt einer Direktwerbung bereits widersprochen?

Sofern Sie diese bereinigte Empfängerliste verwenden, sollte einem datenschutzkonformen Weihnachtsgruß nichts mehr im Wege stehen.

Jessica Stehn-Bäcker

Magistra Juris, CIPP/E
Senior Consultant Datenschutz, externe Datenschutzbeauftragte

Telefon: +49 40 22861374
E-Mail: js@beredi-datenschutz.de

DSGVO-Konformität allein macht noch kein geruhsames Weihnachten

Alexander Hausner und Jutta Köhn

Ausgangslage

Viele (Cloud-)Software-Anbieter werben auf ihren Internet-Seiten mit der Schlagzeile, dass ihr Produkt DSGVO-konform sei.

Es ist schön und gut und wichtig für den verantwortlichen und verantwortungsbewussten Anwender, dass Unternehmen sich seit dem Inkrafttreten der DSGVO aktiv um deren Einhaltung bemühen und dies den (potenziellen) Anwendern auch transparent machen. Das sollte aber nicht davon ablenken, dass der deutsche Gesetzgeber weitere Anforderungen an IT-Systeme in verschiedenen Gesetzen und Regelwerken formuliert hat, die es einzuhalten gilt. In manchen Fällen ergänzen sich diese Anforderungen, sodass Maßnahmen mehrere gesetzliche Anforderungen gleichzeitig bedienen. In manchen Fällen kann es aber auch zu Zielkonflikten führen. Die Verantwortung, dieses auszuloten, liegt immer bei dem Unternehmen, welches eine Software bzw. ein IT-System nutzt.

In der heutigen Ausgabe von SEC.PRO LOG wollen wir uns dem § 146 Abs. 2 AO (Abgabenordnung) in zwei Fällen widmen: der Nutzung eines Software-Produktes zur Finanzbuchhaltung, Personalverwaltung oder Reisekostenabrechnung als Service (SaaS), zusammen mit dem Fall, dass ein Unternehmen oder der Software-Anbieter Hardware-Ressourcen als Service (HaaS) nutzt.

Was fordert § 146 Abs. 2 AO?

§ 146 AO bezieht sich auf Ordnungsvorschriften für die Buchführung und für Aufzeichnungen.

Gemäß § 146 Abs. 2 AO sind Bücher und Aufzeichnungen (Buchführung) im Geltungsbereich der AO zu führen und aufzubewahren. Für bestimmte Betriebsstätten außerhalb des Geltungsbereiches der AO kann es Ausnahmen geben. Im Geltungsbereich der AO heißt dies: Der Ort der Buchführung muss sich auf deutschem Hoheitsgebiet befinden. Der Gesetzgeber unterscheidet dabei zunächst nicht, ob die Bücher in Papierform oder in elektronischer Form geführt werden.

§ 146 Abs. 2a enthält eine Verlagerungsmöglichkeit insoweit, als dass die Finanzbehörde abweichend zu Abs. 2 Satz 1 auf **schriftlichen Antrag des Steuerpflichtigen** hin bewilligen kann, dass unter bestimmten Voraussetzungen elektronische Bücher und sonstige erforderliche elektronische Aufzeichnungen oder Teile davon außerhalb des Geltungsbereichs dieses Gesetzes geführt und aufbewahrt werden können.

Werden der Finanzbehörde Umstände bekannt, die zu einer Beeinträchtigung der Besteuerung führen, hat sie die Bewilligung zu widerrufen und die unverzügliche Rückverlagerung der elektronischen Bücher und sonstigen erforderlichen elektronischen Aufzeichnungen in den Geltungsbereich dieses Gesetzes zu verlangen.

§ 146 Abs. 2b beschreibt mögliche monetäre Konsequenzen für den Steuerpflichtigen. Das Finanzamt kann in folgenden Fällen ein Verzögerungsgeld von 2.500 bis 250.000 Euro festsetzen:

- Eine Verlagerung der Buchführung ist ohne vorherige Bewilligung durch das zuständige Finanzamt erfolgt,
- der Datenzugriff im Rahmen einer steuerlichen Außenprüfung gemäß § 147 Abs. 6 AO wird nicht pflichtgemäß (fristgerecht und in geforderter Art und Weise sowie Umfang) ermöglicht,
- eine geforderte Rückverlagerung der Buchführung ist nicht erfolgt,
- der Standort des Datenverarbeitungssystems und/oder der Name und/oder die Anschrift eines beauftragten Dritten wurden geändert und dem Finanzamt nicht mitgeteilt,
- die Besteuerung wird beeinträchtigt.

Als Voraussetzung für eine Bewilligung einer Verlagerung wird verlangt, dass

- der Steuerpflichtige der zuständigen Finanzbehörde den Standort des Datenverarbeitungssystems und bei Beauftragung eines Dritten dessen Namen und Anschrift mitteilt,
- der Steuerpflichtige seinen übrigen Mitwirkungspflichten nach der AO (§§ 90, 93, 97, 140 bis 147 und 200 Absatz 1 und 2) ordnungsgemäß nachgekommen ist,
- der Datenzugriff durch die Finanzbehörde (nach § 147 Absatz 6) in vollem Umfang möglich ist und
- die Besteuerung hierdurch nicht beeinträchtigt wird.

Was bedeutet das für den Steuerpflichtigen?

§ 146 AO verlangt, dass bei **Buchhaltung in Papierform** die Aufbewahrung der Papierbücher und -aufzeichnungen nicht außerhalb der Gültigkeit der AO erfolgen darf. Führt ein Steuerpflichtiger seine Bücher in Papierform, dürfen Originalaufzeichnungen den Gültigkeitsbereich der AO nicht verlassen. Es ist aber zulässig, Kopien (Papierbelege oder digitale Belege) zu versenden. Umstritten ist, inwieweit der Begriff des „Führens" einer Papierbuchhaltung eine elektronische Datenverarbeitung im Ausland ermöglicht, ohne eine Bewilligung i. S. d. § 146 Abs. 2a zu benötigen. Es wird in der Fachliteratur teilweise als zulässig erachtet, bestimmte Teile des Buchführungsprozesses standortunabhängig fremd zu vergeben, beispielsweise die Erfassung von Geschäftsvorfällen in ein Anwendungssystem. Auch eine Kontierung soll im Ausland auf Kopien von Belegen möglich sein.

Ein Steuerpflichtiger kann, wenn der Speicherort seiner elektronischen Bücher nicht im Geltungsbereich der AO liegen soll, bei der für ihn zuständigen Finanzbehörde einen schriftlichen Antrag auf Bewilligung der Verlagerung der elektronischen Buchführung stellen. Die **Antragstellung** muss in jedem Fall **vor dem Beginn der Verlagerung** erfolgen und eine **Verlagerung** darf **erst nach Vorliegen einer Bewilligung** durch die zuständige Finanzbehörde begonnen werden, andernfalls muss sich der Speicherort der Daten, d. h. der physische Standort der Datenhaltung (Speicher-, Hardware-Komponenten) im Geltungsbereich der AO befinden.

Berührungspunkte von DSGVO und anderen Regularien zur Buchführung (HGB, AO, GoBD)

Die DSGVO ist eine EU-Verordnung und gilt für personenbezogene Daten. Die AO ist ein Gesetz des deutschen Finanzministeriums und gilt für steuerrelevante Daten. Insofern hat eine Aussage über DSGVO-Konformität keine Relevanz für die steuerrechtlichen Anforderungen.

Die in der DSGVO geforderten technisch-organisatorischen Maßnahmen (TOMs) decken einige der Anforderungen der GoBD ab. Beispielsweise geforderte Maßnahmen zum Schutz der Daten vor Verlust (Diebstahl, Vernichtung, Unauffindbarkeit) sowie gegen unberechtigte Eingaben und Änderungen (Berechtigungskonzept etc.) sind für die GoBD ebenso relevant.

Andere Anforderungen der GoBD/des HGB an **Aufbewahrungsdauern**, **Datenzugriff und die Auswertbarkeit** werden nicht durch Maßnahmen im Rahmen der DSGVO abgedeckt.

Auch die Nichteinhaltung der GoBD kann zu Konsequenzen führen: Sind die **Nachvollziehbarkeit und Nachprüfbarkeit** beeinträchtigt, kann durch das zuständige Finanzamt ein formeller Mangel mit sachlichem Gewicht festgestellt werden, der zum Verwerfen der Buchführung führen kann.

Was ist bei der Nutzung von SaaS-/Cloud-Lösungen zu beachten?

Anwendungssysteme, die zwar selbst kein Buchführungssysteme sind, jedoch Daten generieren, die als Buchführungsbelege gebucht werden, wie beispielsweise ein Anwendungssystem für die Reisekostenabrechnung oder eine Personalabrechnungssoftware, sind gemäß den „Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)" des Bundesministeriums der Finanzen als „Vorsystem" oder „Nebenbuch" zu betrachten und somit steuerrelevant, d. h. unterliegen der AO.

Planen Sie die Nutzung einer Cloud-Lösung (SaaS) für Daten, die als steuerlich relevant einzustufen sind, ist die wichtigste Frage folglich die nach dem **Ort der Datenhaltung**. Dabei sind folgende Fälle zu unterscheiden:

Fall A

Verarbeitet und speichert der Software-Anbieter die Daten in seinem eigenen Haus auf eigenen physischen Servern und in einem im deutschen Hoheitsgebiet befindlichen Rechenzentrum? Wenn ja, ist im Hinblick auf die AO dieser Punkt in Ordnung. Wir empfehlen, eine verbindliche Bestätigung vom Anbieter anzufordern, die auch Gültigkeitszeiträume enthält. Datenschutzrechtlich wird der Software-Anbieter regelmäßig Auftragsverarbeiter sein. Wenn der Anbieter DSGVO-Konformität zusichert, ist dies ein echter Mehrwert, denn die technisch-organisatorischen Maßnahmen (TOMs) decken auch viele technische Anforderungen der GoBD ab.

Fall B

Bedient sich der Software-Anbieter einer Cloud-Hardware-Lösung (HaaS)? Dann lautet die Frage, an welchem Ort sich die genutzten Hardware-Ressourcen physisch befinden. Nach unseren Recherchen betreiben einige große Anbieter von Rechner- und Speicherressourcen in Deutschland (im

Geltungsbereich der AO) keine physische Hardware, sondern nur im Bereich der EU. Will man ein Produkt dieses Anbieters nutzen, ist es unbedingt erforderlich, vor dem Nutzungsbeginn bei der zuständigen Finanzbehörde einen **Antrag auf Bewilligung** der Verlagerung zu stellen und die Bewilligung abzuwarten. Datenverarbeitung in der EU liegt im Anwendungsbereich der DSGVO.

Fall C

Bedient sich der Software-Anbieter einer Cloud-Hardware-Lösung (HaaS) und würde die Datenspeicherung außerhalb der EU erfolgen, ist es ebenfalls unbedingt erforderlich, vor dem Nutzungsbeginn bei der zuständigen Finanzbehörde einen Antrag auf Bewilligung der Verlagerung zu stellen und die Bewilligung abzuwarten. Zusätzlich sind dann auch datenschutzrechtliche Aspekte hinsichtlich der Verarbeitung von personenbezogenen Daten zu berücksichtigen, insbesondere ob das Datenschutzniveau des Drittlandes der DSGVO entspricht.

Fall D

Ein Unternehmen betreibt keine Server/Hardware im eigenen Haus, sondern möchte eine Hardware-Lösung HaaS nutzen. Dann ist mit dem Anbieter zu klären, wo sich der Standort der Hardware befindet. Zu beachten ist gegebenenfalls, ob der Anbieter über eigene Hardware-Ressourcen verfügt oder selbst nur als Zwischenhändler agiert. Ggf. sind eine steuerrechtliche Bewilligung sowie eine datenschutzrechtliche Absicherung des Datenschutzniveaus erforderlich.

Praxistipps

Wenn Sie planen, eine Cloud-Software zu nutzen, in denen steuerrelevante Daten verarbeitet werden sollen, lassen Sie sich von dem potenziellen Anbieter über Folgendes verbindlich informieren:

- Wenn mit DSGVO-Konformität geworben wird: Wer hat die Prüfung durchgeführt und wie und was wurde geprüft?
- Sind die Anforderungen der AO, insbesondere der Standort der Datenspeicherung sowie Verarbeitung, sowohl durch den Anbieter als auch durch dessen Auftragnehmer erfüllt? Wenn ja, mit welchen Maßnahmen wurde das erreicht?
- Sind die Anforderungen an Datensicherheit, Auswertbarkeit und Zugreifbarkeit gemäß GoBD erfüllt und wenn ja: Mit welchen Maßnahmen wurde das erreicht?
- Wie wird sichergestellt, dass alle relevanten Anforderungen über den erforderlichen Zeitraum erfüllt werden und bis zum Ablauf der einzuhaltenden Aufbewahrungsfristen erfüllt bleiben?
- Wie erfährt der Anwender zeitnah, wenn der Anbieter Änderungen seiner AGBs vornimmt, die unerwünschte Auswirkungen auf die zuvor zugesagten Eigenschaften haben?

Hilfestellung zu diesen Themen leisten wir Ihnen jederzeit gerne. Sprechen Sie uns an.

Alexander Hausner LL. M.

Rechtsanwalt, Fachanwalt für Arbeitsrecht, zert. Datenschutzbeauftragter

Telefon: +49 40 4223 6660-0
E-Mail: a.hausner@roser-hamburg.de

Jutta Köhn

IT- and Business Auditor, CISA

Telefon: +49 40 4223 6660-0
E-Mail: j.koehn@roser-hamburg.de

BEREDI Marketing GmbH
Bereich Datenschutz

Überseeallee 1
20457 Hamburg

www.beredi-datenschutz.de
www.beredi.de
Telefon: +49 40 22861374
Telefax: +49 40 22861379

Roser Rechtsanwaltsgesellschaft mbH

Roser GmbH Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

Drehbahn 7
20354 Hamburg

www.roser-group.de
Telefon: +49 40 4223 6660-0
Telefax: +49 40 4223 6660-12