Luther.

Newsletter IP/IT

1. Ausgabe 2021

Inhalt

Datenschutz und Brexit – Auswirkungen des EU-UK Trade and Cooperation Agreement

Großbritannien und die EU haben sich auf ein Handelsabkommen geeinigt, welches auch Regelungen zur grenzüberschreitenden Übermittlung von personenbezogenen Daten enthält.

Hintergrund

In dem „EU-UK Trade and Cooperation Agreement“ vom 24. Dezember 2020 legen die EU und Großbritannien u. a. fest, dass für die grenzüberschreitende Übermittlung der Daten zwischen Großbritannien und der EU eine Übergangszeit gilt, in der Großbritannien datenschutzrechtlich vorerst nicht als Drittland, sondern weiterhin als EU-Mitgliedsland behandelt wird. Dies gilt bis zu dem Zeitpunkt, in welchem die Europäische Kommission einen Angemessenheitsbeschluss für das Königreich erlassen hat oder eine weitere Frist von vier Monaten abgelaufen ist, wobei sich diese Frist automatisch um zwei weitere Monate verlängert, falls keiner der Vertragsparteien der automatischen Fristverlängerung widerspricht.

Übergangszeitraum von maximal sechs Monaten

In dem Abkommen wird festgelegt, dass das datenschutzrechtliche Niveau Großbritanniens zum Zeitpunkt des Abschlusses der Vereinbarung dem Niveau der DSGVO entspricht, weshalb eine Übermittlung personenbezogener Daten zunächst weiterhin zulässig ist. Für den Zeitraum dieser Übergangslösung von maximal sechs Monaten müssen Unternehmen daher keine weiteren Vorkehrungen treffen, um Daten zwischen der EU und Großbritannien transferieren zu können. Wenn die Europäische Kommission innerhalb der Übergangsfrist für Großbritannien einen Angemessenheitsbeschluss erlässt, ändert sich daran auch nach dem Ablauf der Frist nichts.

Angemessenheitsbeschluss absehbar?

Im Vorfeld der Verhandlungen war lange Zeit fraglich, ob die Kommission einen Angemessenheitsbeschluss zu Gunsten Großbritanniens nach dem Brexit erlassen würde. Mit dem britischen “Investigatory Powers Bill” von 2016 und der damit einhergehenden umfassenden Möglichkeit zur Vorratsdatenspeicherung sowie der fehlenden Geltung des EU-US-Privacy-Shield für Datenübermittlungen im Verhältnis zwischen Großbritannien und USA existieren erhebliche Risiken für personenbezogene Daten, die es in dieser Form in der EU bisher nicht gab. Für einen Angemessenheitsbeschluss spricht mittlerweile, dass Großbritannien im Vorfeld des Austritts bereits damit begonnen hat, die Regelungen der DSGVO weitestgehend ins nationale Recht aufzunehmen, um sein datenschutzrechtliches Schutzniveau dem der EU anpassen zu können. Durch das Abkommen scheint der Erlass eines Angemessenheitsbeschlusses nunmehr wahrscheinlich. Die EU stellt jedenfalls klar, dass sie die Umsetzung der Regelungen der DSGVO ins nationale britische Recht grundsätzlich als ausreichend anerkennt, um für einen hinreichenden Schutz der Daten der betroffenen Personen im Rahmen der grenzüberschreitenden Übermittlung der Daten zu sorgen. Das Abkommen besagt allerdings auch, dass dies nur solange der Fall ist, wie Großbritannien nicht von der Umsetzung der Regelungen im nationalen Recht abweicht. In einem solchen Fall soll Großbritannien als Drittland behandelt werden.

Falls kein Angemessenheitsbeschluss ergeht

Erlässt die Europäische Kommission bis zum Ablauf der Übergangsfrist keinen Angemessenheitsbeschluss, müssen Unternehmen auf andere Lösungsansätze ausweichen. In einem solchen Fall bliebe für Unternehmen die Möglichkeit, “geeignete Garantien” nach Artikel 46 DSGVO nachzuweisen. Zu diesen gehören beispielsweise die EU-Standardvertragsklauseln, verbindliche unternehmensinterne Regelungen (“Binding Corporate Rules”, “BCR”) oder Zertifizierungen. All diesen Maßnahmen ist jedoch eins gemeinsam: Sie erfordern proaktives Handeln der datenverarbeitenden Unternehmen. Bestehende Auftragsverarbeitungsverträge müssten geprüft und in Nachverhandlungen gegebenenfalls durch EU-Standardvertragsklauseln ergänzt werden. Diese sind auch heute schon das Mittel der Wahl für grenzüberschreitenden Datenverkehr außerhalb der EU/des EWR. Unternehmensintern müssen BCR neu eingeführt oder (falls bereits vorhanden) bestehende BCR überarbeitet werden. Und für Zertifizierungen muss anhand von Kriterienkatalogen der Aufsichtsbehörden und den Prüfanforderungen der zertifizierenden Stelle nachgewiesen werden können, dass die Verarbeitung personenbezogener Daten in Großbritannien dem Datenschutzniveau der EU entspricht. Zuletzt hätten die Unternehmen nach Artikel 49 der DSGVO u. a. auch die Möglichkeit eine Einwilligung der Betroffenen einzuholen, um die Daten zulässig grenzüberschreitend übermitteln zu können. Dieser Artikel hat jedoch einen Ausnahmecharakter und könnte nur restriktiv und mit hohem unternehmerischen Aufwand angewendet werden.

Unser Kommentar

Unternehmen, die Daten nach Großbritannien übermitteln, sollten die weiteren Entwicklungen auf europäischer Ebene genauestens beobachten. Sobald abzusehen ist, wie die EU über einen möglichen Angemessenheitsbeschluss entscheiden wird, müssen die potenziellen Konsequenzen evaluiert werden. Ergeht kein Angemessenheitsbeschluss, sollte der gesamte Datentransfer nach Großbritannien geprüft und auf eine rechtssicheres Fundament gestellt werden. Hierzu gehört insbesondere der Abschluss von EU-Standardvertragsklauseln; in welcher Form dies erfolgen sollte, ist aber ebenfalls noch offen. Denn die EU-Kommission plant – als Folge des EuGH-Urteils zur Unwirksamkeit des EU-US Privacy Shield („Schrems II“) und der darunter stattfindenden Datentransfers – die Klauseln in diesem Jahr zu überarbeiten. Erste Entwürfe wurden bereits veröffentlicht. Es bleibt jedoch abzuwarten und zu prüfen, ob die Anpassungen der EU-Kommission tatsächlich den gewünschten Effekt haben und Datentransfers außerhalb der EU/des EWR vereinfachen werden.

Datenschutz in den USA – Do Not Sell My Personal Information

„Do Not Sell My Personal Information“ – solch eine Auswahlmöglichkeit müssen Unternehmen, die Geschäfte in Kalifornien machen, auf ihrer Website bereitstellen. Kalifornische Verbraucher erhalten so die Möglichkeit, dem Verkauf ihrer Daten mittels Opt-Out zu widersprechen. Per Volksentscheid wurde am 3. November 2020 ein neues Gesetz verabschiedet, das weitere umfangreiche Verpflichtungen zum Datenschutz mit sich bringt.

Hintergrund: CCPA und CPRA

Bei den US-Wahlen haben die Wähler in Kalifornien auch über eine Reihe von Gesetzesmaßnahmen für ihren Staat mit abgestimmt. Eine der bemerkenswertesten Initiativen (Ballot Initiatives) war die Abstimmung über den California Privacy Rights Act of 2020 (CPRA), der erwartungsgemäß mit einer Mehrheit der Stimmen von den Wählern angenommen wurde.

Der CPRA verleiht den bestehenden Bestimmungen des California Consumer Privacy Act (CCPA) mehr Gewicht und ergänzt sie. Er wird deswegen auch CCPA 2.0 genannt. Der zu Beginn des Jahres 2020 in Kraft getretene CCPA war der Wegweiser in Sachen Datenschutz in den USA. Die Regelungen des CPRA spiegeln nun einen großen Teil der Vorschriften der europäischen DSGVO wider. Mit Inkrafttreten des CPRA im Januar 2023 rücken die kalifornischen Datenschutzbestimmungen dadurch noch ein großes Stück näher an die DSGVO-Standards heran.

Neue Kategorie von sensiblen persönlichen Informationen

Ähnlich wie in der DSGVO werden besonders schutzbedürftige Daten definiert. Hierzu gehören die Sozialversicherungsnummer, aber auch Geolocation, Rasse oder ethnische Herkunft, religiöse Überzeugungen oder biometrische Daten sowie Daten über die sexuelle Orientierung. Für diese Daten werden den betroffenen Personen erweiterte Rechte gewährt, wie z. B. die Beschränkung der Nutzung und Offenlegung dieser Art von Informationen.

Neue Datenschutzbehörde

Vorgesehen ist die Bildung einer eigenständigen Datenschutzbehörde (CDPA), um die Einhaltung des Datenschutzes durchzusetzen. Momentan liegt die Aufsicht beim kalifornischen Generalstaatsanwalt. Die neue Behörde wird Verstöße gegen die datenschutzrechtlichen Pflichten untersuchen und auch sanktionieren können. Daneben soll sie Hinweise zur Anwendung und Umsetzung des CPRA geben.

Verkauf von Daten nicht mehr erforderlich

Eine der wichtigsten Neuerungen ist die Erweiterung des Anwendungsbereichs des CCPA: Zum bisher erfassten „Selling", also Verkaufen von Daten, ist das „Sharing", also das Teilen von Daten zwischen Unternehmen hinzugekommen. Bisher konnten sich Unternehmen dem Anwendungsbereich entziehen, indem sie sich darauf beriefen, persönliche Daten auszutauschen, ohne diese zu verkaufen. Dies wurde bisher als Gesetzeslücke kritisiert und soll sich in Zukunft ändern. Das wird z. B. dann relevant, wenn der Verbraucher sein Opt-Out-Recht geltend machen will; in Zukunft können Verbraucher der Weitergabe ihrer Daten widersprechen, auch wenn diese nicht verkauft werden.

Erweiterte Klagemöglichkeiten für Verbraucher

Bisher stehen kalifornischen Verbrauchern unter bestimmten Voraussetzungen private Klagemöglichkeiten im Falle eines Bruchs der Datensicherheit zu, wenn dies zur Folge hatte, dass bestimmte unverschlüsselte Daten – etwa die Sozialversicherungsnummer – gestohlen wurden. Der CPRA erweitert die Liste der geschützten Daten um E-Mail-Adressen und Passwörter.

Datenschutzprinzipien wie in der DSGVO

Auch begrifflich nähert sich der neue CPRA an die Terminologie der DSGVO an; es werden Datenschutzprinzipien festgelegt wie die Datenminimierung und die Zweckbeschränkung der Datenverarbeitung.

Mehr Rechte für Verbraucher

Nach dem CCPA haben Verbraucher momentan das Recht auf Auskunft über die Verarbeitung ihrer persönlichen Daten, das Recht auf Löschung und Widerspruch (Opt-Out) gegen den Verkauf ihrer Daten. Letzteres wird außerdem erweitert in Bezug auf automatische Entscheidungsfindung inklusive Profiling. Neu hinzu kommt das Recht auf Einschränkung der Verarbeitung von sensiblen persönlichen Daten, das Recht, Informationen zu korrigieren sowie das Recht auf Datenübertragbarkeit.

Ausblick

Das Gesetz tritt Januar 2023 in Kraft und kann ein halbes Jahr später durchgesetzt werden, dann aber rückwirkend für Datenerhebungen ab dem 1. Januar 2022. Spätestens dann sollten Unternehmer, nicht nur mit Sitz in Kalifornien, die Einhaltung der neuen Regelungen sicherstellen können. Andere US-Bundesstaaten werden vermutlich dem Beispiel Kaliforniens folgen. Damit bleibt ein Jahr, um die Anpassung an den neuen CPRA vorzubereiten. Die angedrohten Sanktionen sind zwar deutlich geringer als die nach der DSGVO vorgesehenen Bußgelder, gleichwohl ist das finanzielle Risiko erheblich, da die Strafe je Verstoß und je betroffener Person bis zu USD 7,500 betragen und sich so schnell aufsummieren kann. Hinzu kommen die gerade in den USA sehr relevanten Klagemöglichkeiten der Verbraucher auf Schadensersatz – auch im Wege von Sammelklagen.

Der Schutz von Geschäftsgeheimnissen – angemessene Geheimhaltungsmaßnahmen und inhaltsleere Geheimhaltungsklauseln

Das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) fordert „angemessene Geheimhaltungsmaßnahmen“, damit Geschäftsgeheimnisse auch tatsächlich den gesetzlichen Schutz genießen. Allerdings stellt das Gesetz nur wenige Anhaltspunkte zu der praktischen Umsetzung solcher Maßnahmen bereit. Es ist daher Aufgabe der Gerichte, diese Anforderungen zu konkretisieren.

Hintergrund

Das im April 2019 in Kraft getretene Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) hat eine Diskussion über die Frage in Gang gesetzt, was mit „angemessenen Geheimhaltungsmaßnahmen“ gem. § 2 Nr. 1 GeschGehG gemeint ist. Ein Urteil des Landesarbeitsgericht Düsseldorf (LAG Düsseldorf, Urteil vom 3. Juni 2019, Az. 12 SaGa 4/20) liefert hierzu eine erste wichtige Einschätzung und macht deutlich, wann der Schutz nach dem Gesetz zu versagen ist. Hieraus lassen sich konkrete Anforderungen für die Gestaltung von Geheimhaltungsklauseln ableiten, vor allem jedoch wird deutlich, dass Unternehmen abseits hiervon ganz grundsätzlich effektive Geschäftsgeheimniskonzepte benötigen, da eine „catch all“-Klausel zur Geheimhaltung allein gerade keinen ausreichenden Schutz bieten kann.

Der Sachverhalt

Ein Unternehmen war per einstweiliger Verfügung gegen einen ehemaligen Mitarbeiter vorgegangen und hatte dabei die Verletzung von Geschäftsgeheimnissen behauptet. Der Mitarbeiter war auch nach seinem Ausscheiden im Besitz einer Kundenliste, die über 240 Kunden des Unternehmens, deren Anschriften, abgenommene Mengen eines Produkts und die damit generierten Umsätze enthielt. Daneben hatte er privat (z. B. in seinem privaten Kalender) Aufzeichnungen über Kundentermine, Ansprechpartner sowie Kontaktinformationen und Umsätze angefertigt. Die Informationen hieraus nutzte der ehemalige Mitarbeiter, um im Rahmen seiner neuen Position bei einem Mitbewerber Kunden seines ehemaligen Arbeitgebers anzusprechen.

Das klagende Unternehmen trug vor, sowohl bei der Kundenliste als auch bei den privaten Aufzeichnungen würde es sich um Geschäftsgeheimnisse des Unternehmens handeln und die Nutzung der Informationen hieraus stelle eine Verletzungshandlung nach dem Geschäftsgeheimnisgesetz dar. Es bezog sich zur Darlegung angemessener Schutzmaßnahmen ausschließlich auf eine vertragliche Geheimhaltungspflicht, nach der „*alle Angelegenheiten und Vorgänge, die im Rahmen der Tätigkeit bekannt werden*“ vom Mitarbeiter geheim gehalten werden sollten. Derartige „catch all“-Klauseln sind tatsächlich im Bereich des Geheimnisschutzes in vielen Arten von Vertragsdokumenten weit verbreitet.

Die Entscheidung

Das LAG Düsseldorf stellte in seinem Urteil zunächst fest, dass vertragliche Vereinbarungen zwar durchaus ein Mittel des Geheimnisschutzes darstellen können. Es machte jedoch im vorliegenden Fall deutlich, dass die Regelungen zur Geheimhaltungspflicht aus dem Arbeitsvertrag „*deutlich zu weitgehend*“ und darüber hinaus auch „*inhaltsleer*“ seien. Diesen fehle jeglicher Bezug zu dem Begriff des Geschäftsgeheimnisses im Sinne des Rechts, die Klausel würde sogar ausdrücklich das erfassen, was kein Geschäftsgeheimnis sei. Das Gericht resümierte deshalb, § 2 Nr. 1 lit. b) GeschGehG würde seines Inhalts und Zwecks entleert, ließe man eine solche Regelung ausreichen. Es entschied dementsprechend, dass es betreffend die Kundenliste an angemessenen Geheimhaltungsmaßnehmen des Unternehmens gefehlt habe. Dabei berücksichtigte es auch, dass der ehemalige Arbeitgeber Kenntnis davon hatte, dass sich die Kundenliste nach dem Ausscheiden des Mitarbeiters noch in seinem Besitz befand, diese jedoch nicht zurückforderte. Dies spreche ebenfalls dafür, dass kein aktiver Geheimnisschutz vorliege.

Was die privaten Aufzeichnungen des ehemaligen Mitarbeiters betrifft, so seien diese Gegenstand ausreichender Schutzmaßnahmen gewesen, da arbeitsvertraglich für den Fall der Beendigung des Arbeitsverhältnisses die Rückgabe von dienstlichen Unterlagen und durch den Mitarbeiter angefertigten „*Aufzeichnungen und Gesprächsunterlagen*“ geregelt war und die Aufzeichnungen damit konkret bezeichnet wurden. Die Tatsache, dass das Unternehmen auch in diesem Fall keine Herausgabe der entsprechenden Dokumente vom Mitarbeiter verlangt hatte, spreche hier nicht gegen einen angemessenen Geheimnisschutz, denn die Existenz der privaten Aufzeichnungen sei dem Unternehmen schließlich nicht bekannt gewesen.

Während das LAG Düsseldorf somit Ansprüche aus der Nutzung der Kundenliste verneinte, sprach es dem Unternehmen Unterlassungsansprüche aus den privaten Aufzeichnungen des ehemaligen Mitarbeiters zu.

Unser Kommentar

Das Urteil macht deutlich, dass allgemein gefasste Geheimhaltungsklauseln nicht dazu geeignet sind, einen angemessenen Schutz von geschäftlichem Know-how im Unternehmen zu begründen. Gerade die in vielen Verträgen anzutreffenden Formulierungen, die eine Erstreckung auf möglichst alle im Unternehmen vorhandenen Informationen erreichen sollen, können dazu führen, dass wirksamer Schutz nach dem Geschäftsgeheimnisgesetz gar nicht erst entsteht. Dies gilt jedenfalls dann, wenn andere angemessene Schutzmaßnahmen nicht getroffen wurden.

Unternehmen sind gut beraten, abseits einer isolierten Betrachtungsweise von einzelnen Vertragsklauseln ein funktionierendes Konzept zum Schutz von Geschäftsgeheimnissen zu etablieren. Dabei sollten schützenswerte Informationen zunächst identifiziert, kategorisiert und sodann auch protokolliert werden. Anhand des hierdurch entstehenden Gesamtbildes können sodann geeignete Schutzmaßnahmen eingeführt werden, von denen vertragliche Geheimhaltungspflichten nur einen, wenn auch durchaus kritischen Eckpfeiler darstellen können. Daneben spielen jedoch andere Aspekte, z. B. technische und organisatorische Maßnahmen und arbeitsrechtliche Schutzmechanismen, eine wichtige Rolle. Sind die Geschäftsgeheimnisse eines Unternehmens einmal zutreffend identifiziert und eingeordnet worden, so dürfte die Formulierung geeigneter Geheimhaltungspflichten leicht von der Hand gehen. Denn wie sich aus dem Urteil des LAG Düsseldorf ergibt, geht es hier gerade darum, die Geschäftsgeheimnisse, für die Schutz beansprucht werden soll, möglichst konkret zu benennen.

Das Urteil des LAG Düsseldorf ist im Volltext abrufbar unter: https://www.lag-duesseldorf.nrw.de/beh_static/entscheidungen/entscheidungen/saga/0004-20.pdf

Starke Kundenauthentifizierung via Apps – wer übernimmt Verantwortung für personenbezogene Daten?

Zahlungsdienstleister müssen spätestens seit Ende des Jahres 2020 im Online-Zahlungsverkehr eine „starke Kundenauthentifizierung“ umsetzen. Die von der BaFin eingeräumte Karenzzeit ist ausgelaufen. Um weiterhin rechtskonform zu agieren, müssen neben den Vorgaben aus der Zahlungsdiensterichtlinie PSD 2 (Payment Services Directive II), die sich nun größtenteils im Gesetz über die Beaufsichtigung von Zahlungsdiensten (ZAG) wiederfinden, insbesondere auch allgemeine datenschutzrechtliche Anforderungen bei der Einbindung von Authentifizierungs-Apps beachtet werden.

Rechtsrahmen

Am 14. September 2019 ist das zweite Umsetzungsgesetz der Zahlungsdiensterichtlinie PSD2 in Kraft getreten. Dabei wurden insbesondere Vorschriften im ZAG angepasst. Die Änderungen sollen zu einer höheren Sicherheit im Online-Zahlungsverkehr beitragen und neuen Betrugsmethoden entgegenwirken. Als entsprechende Maßnahme sieht das Gesetz vor, dass Zahlungsdienstleister zu einer “starken Kundenauthentifizierung” verpflichtet werden. Mit Inkrafttreten des Umsetzungsgesetzes sollte die starke Kundenauthentifizierung für alle Online-Zahlungen verpflichtend sein. Jedoch gab die BaFin in einer Pressemitteilung vom 17.10.2019 bekannt, dass bis zum 31.12.2020 eine Karenzzeit für Zahlungsdienstleister mit Sitz in der Bundesrepublik gelte, während der eine Beanstandung durch die BaFin zunächst nicht zu fürchten sei.

Das Ende dieser Karenzzeit ist nun erreicht, doch es verbleiben Unsicherheiten bei Unternehmen, die von der PSD2 betroffen sind. Denn beispielweise müssen bei der Umsetzung der starken Kundenauthentifizierung nicht nur die Finanzsektor-spezifischen Anforderungen, sondern auch weitere gesetzliche Regelungen berücksichtigt werden, wie etwa die Vorgaben der Datenschutz-Grundverordnung (DSGVO). Dies betrifft insbesondere und auch die Zusammenarbeit zwischen Zahlungsdienstleistern und anderen Anbietern, um den sog. zweiten Faktor im Rahmen der Authentifizierung verfügbar zu machen. Werden etwa die Verantwortlichkeiten nicht ordnungsgemäß erfasst und den betroffenen Personen mitgeteilt, können erhebliche Bußgelder durch die Datenschutzaufsichtsbehörden die Konsequenz sein.

Grundlagen der datenschutzrechtlichen Verantwortlichkeit

Im ZAG finden sich keine Regelungen zur datenschutzrechtlichen Verantwortlichkeit bei der Verarbeitung von personenbezogenen Daten, sodass die allgemeinen datenschutzrechtlichen Regelungen anwendbar sind. Die DSGVO unterscheidet im Hinblick auf Datentransfers im Wesentlichen zwischen drei Fallkonstellationen: die Übermittlung zwischen zwei separat Verantwortlichen (Controller-Controller), die Auftragsverarbeitung nach Art. 28 DSGVO (Controller-Processor) sowie die gemeinsame Verantwortlichkeit nach Art. 26 DSGVO (Joint Controllership).

Verantwortlicher ist nach Art. 4 Nr. 7 DSGVO die natürliche oder juristische Person oder andere Stelle, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Eine gemeinsame Verantwortlichkeit liegt vor, wenn die Entscheidung über die Zwecke und Mittel gemeinsam mit anderen erfolgt. In Abgrenzung dazu verarbeitet der Auftragsverarbeiter die Daten lediglich im Auftrag des Verantwortlichen und hat keine Entscheidungsgewalt über die Zwecke, sondern ist vielmehr an die Weisungen des Verantwortlichen gebunden. Die Grenze zwischen den einzelnen datenschutzrechtlichen Rollen ist dabei jedoch häufig schwierig zu ziehen, sodass grundsätzlich jede Übermittlung einzeln und genau bewertet werden muss.

Als Indiz kann dabei die Vereinbarung zwischen den Parteien herangezogen werden, wobei jedoch die tatsächlichen Umstände, also die tatsächliche technische Ausgestaltung der Verarbeitungsprozesse, maßgeblich sind. Das bedeutet, dass, auch wenn die Parteien einen Auftragsverarbeitungsvertrag schließen, tatsächlich aber der „Auftragsverarbeiter“

eigene Zwecke bei der Datenverarbeitung verfolgt, keine Auftragsverarbeitung, sondern vielmehr eine gemeinsame oder separate Verantwortlichkeit der Parteien vorliegt. Diese Bewertung ist insbesondere für die in der DSGVO geregelten Verpflichtungen gegenüber den Betroffenen, wie etwa Informationspflichten, von großer Bedeutung.

Möglichkeiten zur starken Kundenauthentifizierung

Seit Ablauf der Karenzzeit ist eine starke Kundenauthentifizierung für alle Online-Transaktionen Pflicht. Als Online-Transaktionen verstehen sich gemäß § 55 Abs. 1 S. 1 ZAG der Online-Zugriff auf ein Zahlungskonto, das Auslösen eines elektronischen Zahlungsvorganges und jede Remote-Zugriffs-Handlung, die das Risiko eines Betrugs im Zahlungsverkehr oder eines anderen Missbrauchs beinhaltet.

Die starke Kundenauthentifizierung, auch zwei-Faktor-Authentifizierung genannt, bedeutet, dass Online- und Kartenzahlungen in der Regel durch zwei unabhängige Faktoren bestätigt werden müssen. Dabei sind Merkmale aus den Kategorien Wissen (z. B. PIN, Passwort), Besitz (z. B. Handy, Karte, TAN-Generator) und Inhärenz (z. B. Fingerabdruck) denkbar.

Bei der Auslösung eines elektronischen Zahlungsvorganges besteht die Besonderheit, dass die Authentifizierung einen dynamischen Faktor umfassen muss. Wird also beispielsweise als Authentifizierungsfaktor eine TAN (Transaktionsnummer) verlangt, ist es notwendig, dass die TAN im Wege eines dynamischen TAN-Verfahren generiert wird – das heißt, in einem Verfahren, bei dem für jede Transaktion eine neue TAN generiert wird.

Dafür werden von den Zahlungsdienstleistern zunehmend Apps verwendet, wobei jedoch unterschiedliche Authentifizierungsmethoden angeboten werden. Bei TAN-Apps ist der Berechnungs-Algorithmus für die TAN in der Software enthalten. Erhält der Kunde zwei getrennte Apps, eine für das Online-Banking und eine für die starke Kunden-Authentifizierung, muss die TAN für die zu autorisierenden Vorgänge in die andere App übertragen werden, was in der Regel über eine App2App Kommunikation erfolgt. Das funktioniert allerdings bei Multibanking-Apps nicht. Daher erhält man mit neueren Apps über das Smartphone als separaten Kanal eine Push-Nachricht und erteilt die Freigabe über ein biometrisches Merkmal wie den Fingerabdruck oder tippt eine PIN ein. Bei neueren Smartphones kann auch die Consumer Device Cardholder Verification Method (CDCVM) für den Zugriff auf das Gerät und für die Authentifizierung von Zahlungen – insbesondere für mobile Near Field Communication (NFC)-Zahlungen – genutzt werden. Hierzu muss das Gerät samt CDCVM auf den Inhaber vorab registriert werden.

Datenschutzrechtliche Verantwortlichkeit bei Authentifizierungs-Apps

In eine Zahlung im Rahmen einer Online-Transaktion können eine Bank, ein Kreditkartenunternehmen, Internetbezahlverfahren (wie Sofort Überweisung) oder mobile Bezahlverfahren (wie Apple und Google Pay) als Zahlungsdienstleister eingebunden sein. In manchen Angeboten übernimmt ein weiterer Zahlungsdienstleister die Integration unterschiedlicher Zahlungsarten in den bestehenden Onlineshop.

Bei der Generierung der TAN via Apps werden von den App-Betreibern Autorisierungsdaten und Transaktionsdaten verarbeitet, sodass sich die Frage nach der datenschutzrechtlichen Verantwortlichkeit für die Verarbeitung sowie der Rechtsgrundlage für die Übermittlung der Transaktionsdaten stellt. Bei der Verarbeitung dieser Daten sind verschiedene Beteiligte involviert: der Online-Händler, der oder die Zahlungsdienstleister, der Entwickler und der Anbieter der Authentifizierungs-App im App-Store (die identisch sein können, aber nicht müssen), der Betreiber der App und ggf. ein technischer Dienstleister.

Rechtsgrundlage

Zahlungsdienstleister dürfen die personenbezogenen Daten, die für das Erbringen ihrer Zahlungsdienste notwendig sind, ausschließlich mit der ausdrücklichen Einwilligung des Zahlungsdienstnutzers verarbeiten (§ 59 Abs. 2 ZAG), soweit sie diese Daten nicht auf gesetzlicher Grundlage zur Verhütung, Ermittlung und Feststellung von Betrugsfällen im Zahlungsverkehr notwendigerweise verarbeiten (§ 59 Abs.1 ZAG). In diesem Zusammenhang hat der Europäische Datenschutz-

ausschuss mit seinen Leitlinien 06/2020 über das Zusammenspiel von PSD2 und DSGVO klargestellt, dass es sich bei dieser Einwilligung um eine solche vertraglicher Natur und nicht um eine Einwilligung im engen Sinne der DSGVO handelt. Von einem Zahlungsdienstleister mit der Erbringung von Authentifizierungsleistungen beauftragte Dienstleister dürfen die Daten nach den allgemeinen Regelungen der DSGVO nur nach Weisung des jeweiligen Zahlungsdienstleisters auf der Grundlage einer Auftragsverarbeitung oder mit ausdrücklicher Einwilligung des Zahlungsdienstnutzers zur Verarbeitung übermittelt erhalten.

Datenschutzrechtliche Verantwortlichkeit und Informationspflichten

Zahlungsdienstleister, die über eine eigene Vertragsbeziehung mit dem Kunden jenseits des konkreten Online-Bezugs- und Bezahlvorgangs verfügen, verarbeiten Daten in ihrer Rolle als Verantwortliche im Sinne von Art. 4 Abs. 7 DSGVO und können ihre selbständigen Informationspflichten in diesem Rahmen erfüllen. Bei Zahlungsdienstleistern, die erst im Rahmen des Online-Bezahlvorgangs eingebunden werden, ist im Einzelfall zu prüfen, ob sie die Kundendaten unmittelbar als Verantwortlicher erheben und wie sie ihren Informationspflichten – etwa durch Ergänzung der Endkundendatenschutzhinweise des Händlers – nachkommen können. Inwieweit Anbieter von Authentifizierungs-Apps im Rahmen des App-Stores eine eigenständige Rechtsbeziehung mit den Kunden eingehen und die ihnen im Rahmen der Autorisierung von Transaktionen zur Verfügung gestellten Daten als selbständig Verantwortliche verarbeiten, wird für Kunden nicht immer ganz deutlich.

In den vertraglichen Vereinbarungen der App-Stores übertragen die App-Store-Betreiber die datenschutzrechtliche Verantwortlichkeit für Apps regelmäßig vollumfänglich auf die Anbieter der App. Beispielsweise heißt es bei den Bedingungen von Google: „*Der Entwickler versichert und garantiert, dass er für die Einhaltung aller anwendbaren Gesetze und Bestimmungen weltweit allein verantwortlich ist*“. Entwickler meint in diesem Fall jedoch nicht den Entwickler im engeren Sinne, sondern denjenigen, der die Rolle des Entwicklers durch das Anbieten der App im App-Store übernimmt. Ein ähnlicher Passus findet sich auch in den Bedingungen von Apple. Allein aus diesen Formulierungen kann jedoch noch nicht geschlossen werden, dass der Anbieter tatsächlich Verantwortlicher im Sinne der DSGVO ist, da dies von der tatsächlichen technischen Ausgestaltung der Verarbeitungsprozesse abhängig ist. Vielmehr ist also entscheidend, wer die Mittel und insbesondere die Zwecke der Verarbeitung bindend festlegen kann.

Das bedeutet, dass also ein App-Anbieter, der aus tatsächlicher Sicht keinen Einfluss auf die Zwecke und Mittel der Verarbeitung hat, regelmäßig nicht Verantwortlicher im Sinne der DSGVO sein kann. Im Umkehrschluss gilt, dass derjenige Anbieter, der über Zwecke und Mittel der Verarbeitung entscheidet, als Verantwortlicher zu qualifizieren ist.

Soweit der Zahlungsdienstleister also nicht selbst Anbieter der Authentifizierungs-App im App-Store ist, hat er offenzulegen, ob der Anbieter der App die Daten als (selbständig oder sog. gemeinsam) Verantwortlicher erhält und verarbeitet. In diesem Fall hat der Zahlungsdienstleister die ausdrückliche Einwilligung der Zahlungsdienstnutzer in die Übermittlung der Transaktionsdaten einzuholen. Entsprechend müssen die Datenschutzhinweise des Zahlungsdienstleisters und die von diesem eingeholten Erklärungen des Zahlungsdienstnutzers sowie die vom App-Anbieter im App-Store veröffentlichten Datenschutzhinweise aufeinander abgestimmt sein. Alternativ kann der Zahlungsdienstleister den App-Anbieter auf Basis einer Auftragsverarbeitung einbinden, wenn ihm die Weisungsbefugnis über Zwecke und Mittel der Verarbeitung durch den App-Anbieter zustehen. Auch dies ist in den jeweiligen Datenschutzhinweisen konsistent abzubilden.

Praxishinweis

Wird Kunden im digitalen Zahlungsverkehr eine Authentifizierungs-App zur Verfügung gestellt, muss zwingend überprüft werden, welche konkreten Datenverarbeitungsvorgänge stattfinden und welche Parteien in welchem Umfang beteiligt sind. Maßgeblich sind dabei die vertraglichen Absprachen und tatsächlichen Umstände. Nachdem die Einflussmöglichkeiten der Beteiligten auf die Datenverarbeitungsvorgänge erfasst wurden, sollten vertragliche Vereinbarungen zwischen den Parteien getroffen werden – das bedeutet ggfs. also auch ein Joint-Controller-Agreement oder ein Auftragsverarbeitungsvertrag. Sobald dann die Verantwortlichkeiten und somit auch die Rechte und Pflichten der Parteien geregelt sind, sind diese den Betroffenen in den Datenschutzhinweisen kenntlich zu machen.

Unlautere Werbung bei Social Media Likes

Mittlerweile ist weitgehend bekannt, dass das Ankaufen von Likes und Bewertungen für Social Media Auftritte von Unternehmen rechtswidrig ist. Es gibt jedoch auch Fallkonstellationen, in denen nicht direkt ersichtlich ist, dass ein „Gefällt mir" unlauter gewonnen wurde. Wichtig ist, dass Likes und Bewertungen für das auf einer Social Media Seite werbende Unternehmen, freiwillig und ohne eine Belohnung des Nutzers abgegeben werden.

Hintergrund

Likes und Bewertungen auf Social Media gewinnen für das Marketing von Unternehmen immer mehr an Bedeutung. Sie sind ein Maßstab für die Bekanntheit und Beliebtheit eines Unternehmens bzw. dessen Produkte und steigern die Reichweite der dort veröffentlichten Beiträge. Kein Wunder also, dass viel getan wird, um hohe Interaktions- und Bewertungs-Zahlen zu erreichen.

Bei Empfehlungen in der Werbung gehen die Nutzer regelmäßig davon aus, dass diese von neutralen Dritten abgegeben wurden, aus den Gründen, die in der Empfehlung genannt sind. Der gleiche Maßstab ist bei Social Media Seiten und deren Likes und Bewertungen zu berücksichtigen. Weichen diese von den genannten Nutzererwartungen ab, so kann es sich um eine unlautere und damit rechtswidrige Irreführung nach dem Gesetz gegen den unlauteren Wettbewerb (UWG) handeln. Diese Rahmenbedingungen werden in den folgenden zwei Beispielen aus der Rechtsprechung näher erläutert.

Gewinnspielteilnahme als Belohnung für Bewertungen

„*Wie du gewinnen kannst? Ganz einfach: Diesen Post liken, kommentieren, teilen; unsere Seite liken oder bewerten. Jede Aktion erhält ein Los und erhöht deine Gewinnchance*" – so warb ein Unternehmen für sein Gewinnspiel und unterlag damit in einem darauffolgenden Rechtsstreit (OLG Frankfurt, Urteil vom 20.8.2020 – 6 U 270/19). Das OLG Frankfurt bestätigte die Auffassung der Vorinstanz, dass die Werbung mit den aus solch einer Aktion resultierenden Bewertungen eine Fehlvorstellung über die Beliebtheit des Unternehmens hervorrufen kann und somit eine Irreführung darstelle. Das Gericht geht in seiner Entscheidung davon aus, dass die Bewertungen durch die Gewinnspielteilnahme beeinflusst werden und dadurch gegebenenfalls positiver ausfallen. Die Besonderheit zu anderen Verfahren ist, dass für die Bewertungen keine direkte Gegenleistung (z. B. durch Gutscheine, Rabatte) geleistet wurde. Bereits die Möglichkeit der Teilnahme am Gewinnspiel wurde durch das Gericht als „Gegenleistung" gewertet.

Nach Auffassung des OLG Frankfurt musste der Kläger nicht alle Bewertungen aufzählen, die auf der Irreführung basieren. Es genügte bereits, dass die Klägerin dies für zwei Bewertungen nachwies. Dann treffe den Seitenbetreiber die Pflicht, darzulegen, dass keine weiteren Bewertungen auf das Gewinnspiel zurückzuführen seien.

Übernahme von Likes bei Unternehmensänderung

Ein weiteres wichtiges Kriterium ist, dass Likes und Bewertungen für das Unternehmen bzw. die Produkte abgegeben wurden, die auf der Social Media Seite genannt sind. So entschied die Rechtsprechung, dass ursprünglich für ein Burger-Restaurant abgegebene Likes nicht für ein, am gleichen Standort eröffnetes, neues Restaurant weiterverwendet werden dürfen (OLG Frankfurt, Urteil vom 14.6.2018 – 6 U 23/17). Der Grund: Dies erwecke die Fehlvorstellung, dass die Likes für das Essen und den Service im neuen Restaurant abgegeben wurden. Denn Facebook bietet die Möglichkeit, eine Seite umzubenennen, ohne dass die für die Seite vorhandenen Likes verloren gehen. Dies hatte die Beklagte getan und so die „alten" Likes weiter für das neue Unternehmen genutzt.

Allein der Vortrag, die Likes könnten nicht einzeln gelöscht werden, führe nicht zu einer anderen Bewertung, so das OLG Frankfurt. Es wies darauf hin, dass es der Beklagten auch zuzumuten sei, die Seite zu löschen und eine eigene, neue Seite zu erstellen, auch wenn hierdurch Likes verloren gehen, die redlich für das neue Restaurant abgegeben wurden.

Unser Kommentar

Da ein Unternehmen mit Likes und Bewertungen auf dem Markt wirbt, kann eine irreführende Verwendung zu Abmahnungen von Mitbewerbern oder Verbraucherverbänden führen. Auf Social Media Seiten sind solche Informationen öffentlich einsehbar, sodass ein Verstoß leicht nachgewiesen werden kann und das Risiko einer Abmahnung steigt. Bei

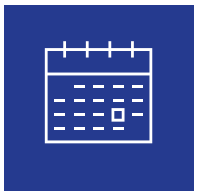
Facebook beispielsweise lässt sich über die Rubrik „Seitentransparenz“ nachverfolgen, ob die Seite zwischendurch umbenannt wurde. Hinzu kommt die Beweiserleichterung, die das OLG Frankfurt aufführt.

Bei Gewinnspielen ist auf die Formulierung zu achten. Eine Kopplung der Abgabe einer Bewertung mit einer Gewinnspielteilnahme sollte unterbleiben. Die bloße Bitte an die Teilnehmer, eine Seite zu bewerten, wird hingegen regelmäßig zulässig sein. Dabei ist aber darauf zu achten, dass dies nicht insofern missverstanden werden kann, dass hierdurch die Gewinnchancen beeinflusst würden.

Das zweite Beispiel wird in der Praxis häufig relevant bei dem Verkauf von Social Media Accounts. Bei Unternehmen der Digitalbranche sind Social Media Kanäle mit hohen Reichweiten wichtige Assets. Insofern ist Vorsicht geboten, wenn hierfür hohe Summen gezahlt werden und dann unter Umständen nicht ohne Weiteres mit den Likes des Vorgängers weiter geworben werden darf, da sich das Unternehmen oder der Unternehmensgegenstand geändert hat.

Die Entscheidungen sind weitgehend auch auf andere Social Media Portale übertragbar, die ebenfalls mit Bewertungssystemen arbeiten. Dabei sollte berücksichtigt werden, dass die Beseitigung rechtswidrig erlangter Likes und Bewertungen durchaus Schwierigkeiten bereiten kann. Je nach Social Media Anbieter können solche Inhalte nicht vom Seitenbetreiber direkt gelöscht werden. Dies kann im Extremfall dazu führen, dass eine gänzlich neue Social Media Präsenz eröffnet werden muss, wodurch weitere Inhalte verloren gehen. Umso wichtiger ist es, beim Betrieb von Social Media Präsenzen von Beginn an die aufgezeigten rechtlichen Maßstäbe zu bedenken.

Veranstaltungen, Veröffentlichungen und Blog



Eine Übersicht mit unseren Veranstaltungen finden Sie hier.

Eine Liste unserer aktuellen Veröffentlichungen finden Sie hier.

Unseren Blog finden Sie hier.

Impressum

Verleger: Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 0
Telefax +49 221 9937 110, contact@luther-lawfirm.com
V.i.S.d.P.: Dr. Michael Rath, Partner
Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 25795
michael.rath@luther-lawfirm.com

Bildnachweis: MR.Cole_Photographer/Getty Images: Seite 1; MicroStockHub/iStock: Seite 3; weyo/ Adobe Stock: Seite 5; AdobeStock: Seite 7; Tomasz Zajda/AdobeStock: Seite 10; bigtunaonline/iStock: Seite 13

Haftungsausschluss

Obgleich dieser Newsletter sorgfältig erstellt wurde, wird keine Haftung für Fehler oder Auslassungen übernommen. Die Informationen dieses Newsletters stellen keinen anwaltlichen oder steuerlichen Rechtsrat dar und ersetzen keine auf den Einzelfall bezogene anwaltliche oder steuerliche Beratung. Hierfür stehen unsere Ansprechpartner an den einzelnen Standorten zur Verfügung.

Luther.

Bangkok, Berlin, Brüssel, Delhi-Gurugram, Düsseldorf, Essen, Frankfurt a. M., Hamburg, Hannover, Jakarta, Köln, Kuala Lumpur, Leipzig, London, Luxemburg, München, Shanghai, Singapur, Stuttgart, Yangon

Weitere Informationen finden Sie unter
www.luther-lawfirm.com
www.luther-services.com