Invisible Payments – aus rechtlicher Sicht spricht nichts dagegen

Von Andreas Walter und Oskar Becker

Die rechtlichen Voraussetzungen für „unsichtbare" Zahlungen sind in Deutschland gegeben, wissen Andreas Walter und Oskar Becker. Nicht alle Zahlungsarten sind dafür jedoch gleichermaßen geeignet. Das gilt beispielsweise aufgrund des Erstattungsrechts für die Lastschrift. Um die Pflicht zur starken Kundenauthentifikation zur erfüllen, nennen die Autoren Zahlungsauslösedienste als gangbaren Weg. Nicht zuletzt gilt es, den Datenschutz zu beachten. Das gilt vor allem dann, wenn der Zahlungsempfänger Daten für Analysen des Kaufverhaltens nutzen will. Red.

Zahlungen, die kassenlos und „unsichtbar" im Hintergrund als automatische Folge der Inanspruchnahme der Hauptleistung oder bei Eintritt sonstiger Bedingungen ausgelöst werden („Invisible Payments"), sind für Zahler und Zahlungsempfänger praktisch, erfordern jedoch eine gründliche Auseinandersetzung mit dem Zahlungsrecht, um in Deutschland durchführbar zu sein.

Um Invisible Payments zu ermöglichen, verwenden Anbieter technische Systeme, um den Kauf eines Produkts oder die Inanspruchnahme von Dienstleistungen einem Zahler zuzuordnen. Hierbei wird auf ein aktives Auslösen der einzelnen Zahlung durch den Käufer verzichtet. Durch die zum Einsatz kommenden technischen Systeme wird die Zahlung automatisch ausgelöst, sobald ein bestimmtes Ereignis eintritt und registriert wird.

Zum Einsatz kommen Invisible Payments beispielsweise bereits in Supermärkten von Amazon Go.[1)] In diesen Supermärkten gibt es keinen klassischen Kassenbereich mehr. Die Kunden weisen sich bei Betreten des Marktes mit ihrer Amazon-App aus. Die Waren, die sie dann im Supermarkt in ihren Einkaufskorb legen, werden mithilfe von Kameras und anderen technischen Systemen automatisch erfasst. Verlässt der Kunde dann den Laden durch die sogenannte „leaving area", werden die Waren dem Amazon-Account des Kunden zugewiesen und automatisch über diesen Account abgerechnet.[2)] Ein separates Auslösen der Zahlung durch den Kunden ist aufgrund der technischen Überwachung des gesamten Einkaufsvorgangs nicht mehr erforderlich. Zukünftig könnte dieses Modell des Einkaufs für den Kunden sogar noch weiter vereinfacht werden, indem die Registrierung bei Betreten des Geschäfts mittels Gesichtserkennung automatisch erfolgt.

Rechtliche Grundlagen des Zahlungsvorgangs

Voraussetzung der Ausführung des Zahlungsvorgangs im Rahmen von Invisible Payments ist, dass die Vertragsparteien vereinbaren, dass mit dem Verlassen des Geschäfts durch den Kunden zum einen ein Kaufvertrag über die aus den Regalen genommenen Waren zustande kommt und dass die Zahlungspflicht des Kunden automatisch erfüllt werden soll, wenn dieser den Supermarkt mit den Waren verlässt.

Bei der dann folgenden Abwicklung des Invisible Payments kommen die bereits etablierten Zahlungsmethoden in Betracht. Unterschiede in der rechtlichen Bewertung im Vergleich zu herkömmlich ausgelösten Zahlungen ergeben sich nur im Hinblick auf die Erteilung des Zahlungsauftrages durch den Kunden.[3)]

Überweisung: Zahlungsauftrag mit Verlassen des Geschäfts

Zunächst kommt eine Abwicklung der Zahlung durch eine Überweisung des geschuldeten Betrages vom Zahlungs-

Prof. Dr. Andreas Walter, Rechtsanwalt, Partner, Schalast LAW | TAX, Frankfurt am Main

konto des Kunden (Zahler) auf das Zahlungskonto des Supermarkts in Betracht. Die Überweisung wird durch einen Zahlungsauftrag gemäß § 675f Abs. 4 S. 2 BGB des Kunden an seinen Zahlungsdienstleister initiiert.

Für die rechtliche Wirksamkeit der Zahlung per Überweisung ist es erforderlich, dass der Zahler der Zahlung zugestimmt hat. Wie diese Zustimmung zu erteilen ist, kann zwischen Zahler und Zahlungsdienstleister vereinbart werden. Im Fall der Invisible Payments müsste eine solche Vereinbarung so ausgestaltet sein, dass der Zahler mit Verlassen des Geschäfts automatisch der Zahlung zustimmt und seinem Zahlungsdienstleister einen Zahlungsauftrag erteilt.

Erstattungsrecht erschwert Nutzung der Lastschrift

Bei der Zahlung mittels Lastschrift erteilt der Kunde dem Supermarkt ein Lastschriftmandat. Dieses ermächtigt den Supermarkt bei entsprechender Gestaltung, den geschuldeten Betrag vom Konto des Kunden bei dessen Zahlungsdienstleister einzuziehen. Darüber hinaus wird der Zahlungsdienstleister des Kunden angewiesen, die vom Supermarkt angefragte Lastschrift einzulösen.[4] Durch dieses Lastschriftmandat hat der Supermarkt die Möglichkeit, dem Zahlungsdienstleister des Kunden einen entsprechenden Zahlungsauftrag zu erteilen, sobald der Kunde das Geschäft verlässt.

Bei der Zahlung per Lastschrift besteht insofern noch eine Besonderheit, dass der Zahler grundsätzlich ein bedingungsloses Erstattungsrecht gegenüber seinem Zahlungsdienstleister hat. Dieses Erstattungsrecht kann der Zahler innerhalb von acht Wochen ab dem Zeitpunkt der Belastung seines Kontos geltend machen. Dann muss der Zahlungsdienstleister dem Zahler den eingezogenen Betrag wieder auf seinem Konto gutschreiben. Der Zahlungsdienstleister hat dann wiederum einen Erstattungsanspruch gegen den Zahlungsempfänger (hier den Supermarkt). Der ursprüngliche Anspruch auf Zahlung des Kaufpreises des Supermarkts gegen den Kunden lebt dann wieder auf und muss vom Supermarkt erneut gegenüber dem Kunden geltend gemacht werden.[5]

Dieses Erstattungsrecht erschwert die Verwendung der Zahlung per Lastschrift im Rahmen von Invisible Payments, da es zu Unsicherheiten für den Supermarkt führt. Gegenüber Personen, die nicht als Verbraucher handeln, kann das Erstattungsrecht allerdings gemäß § 675e Abs. 4 BGB in Verbindung mit § 675x Abs. 4 BGB durch Vereinbarung ausgeschlossen werden.

Zahlung per Kreditkarte erfordert Hinterlegen der Kartendaten

Bei der Zahlung per Kreditkarte sind neben dem Kunden, dessen kartenausgebender Bank und dem Supermarkt (Vertragspartner) noch das Kartenunternehmen und ein Acquirer an der Abwicklung der Zahlung beteiligt.[6] Zwischen dem Supermarkt und dem Karteninhaber (dem Kunden) besteht das Valutaverhältnis, aufgrund dessen der Kunde zur Zahlung an den Supermarkt verpflichtet ist.[7] Zwischen dem Vertragspartner und dem Acquirer besteht ein Akquisitionsvertrag, im Rahmen dessen der Acquirer die vom Kunden geschuldete Zahlung an den Vertragspartner leistet, sobald die Karte zur Zahlung eingesetzt wird.[8] Zwischen dem Acquirer und der kartenausgebenden Bank erfolgt dann im Rahmen des sogenannten Clearingverhältnisses der Ausgleich des von dem Acquirer an den Vertragspartner geleisteten Betrages.[9] Die Bank des Karteninhabers ist aufgrund des zwischen ihr und dem Kunden bestehenden Deckungsverhältnisses verpflichtet, die Weisungen des Karteninhabers umzusetzen, also von diesem autorisierte Zahlungen an den Acquirer zu erstatten.[10]

Die Autorisierung von Zahlungen erfolgt dabei in einem Supermarkt üblicherweise dadurch, dass der Kunde dem Supermarkt seine Kreditkarte vorlegt und die entsprechenden Daten mittels eines Kartenterminals an die kartenausstellende Bank weitergeleitet werden. Dadurch wird dann der Zahlungsvorgang ausgelöst.

Darüber hinaus besteht die Möglichkeit, dass der Kunde seine Kreditkartendaten bereits vor dem Einkauf bei seinem Vertragspartner hinterlegt. Sobald dann ein Einkauf erfolgt, übermittelt der Vertragspartner die entsprechenden Daten an den Acquirer und dieser wiederum an die kartenausgebende Bank. Im Fall der Invisible Payments müsste der Kunde seine Kartendaten vor dem Einkauf beim Supermarkt hinterlegen. Der Supermarkt kann dann den Zahlungsauftrag an den Acquirer weiterleiten, sobald der Kunde den Markt verlässt.

Herausforderung der starken Kundenauthentifizierung

Eine Herausforderung für die Einrichtung eines Invisible-Payment-Systems stellen die gesetzlichen Anforderungen an die starke Kundenauthentifizierungen dar, durch die sichergestellt werden soll, dass ausschließlich der Berechtigte Zahlungen auslösen kann.

Wird ein elektronischer Zahlungsvorgang vom Zahler (Kunden) ausgelöst, ist der Zahlungsdienstleister gemäß § 55 Abs. 1 Nr. 2 ZAG verpflichtet, die starke Kundenauthentifizierung zu verlangen. Diese Authentifizierung muss zwei der drei Elemente – Wissen (etwas, das der Nutzer weiß), Besitz (etwas, das der Nutzer besitzt) und Inhärenz (etwas, das der Nutzer ist) – umfassen. Bei elektronischen Fernzahlungen muss der Zahlungsvorgang zudem dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpft werden.

– Bei Zahlungen per Überweisung müssen die vorgenannten Anforderungen grundsätzlich vollständig erfüllt sein.

– Eine starke Kundenauthentifizierung ist im Falle der Zahlung per Lastschrift grundsätzlich nicht erforderlich, da diese nicht vom Kunden, sondern vom Zahlungsempfänger ausgelöst wird.[11]

– Bei der Zahlung per Kreditkarte an der Kasse am Supermarkt können die

Oskar Becker,
Rechtsanwalt, Schalast LAW | TAX,
Frankfurt am Main

Anforderungen an die starke Kundenauthentifizierung beispielsweise erfüllt werden, indem der Kunde die Karte bei der Zahlung an das Kassenterminal hält (Besitzelement) und seine PIN in das Kartenterminal eingibt (Wissenselement). Eine dynamische Verknüpfung ist nicht notwendig, da der Zahlungsdienstleister den Zahlungsauftrag über das Kassenterminal übermittelt bekommt und dies als Nahzahlung bewertet wird.

Anders sieht dies in den Fällen aus, in denen zwar an der Kasse bezahlt wird, der Zahlungsauftrag jedoch nicht über das Kassenterminal, sondern direkt über das Handy ins Internet an den Zahlungsdienstleister gelangt (zum Beispiel beim Scan eines QR-Codes). Grundsätzlich entspricht dies eher einem elektronischen Fernzahlungsvorgang, sodass hierbei eine dynamische Verknüpfung notwendig ist.

Whitelisting als gangbarer Weg

Es besteht gemäß § 55 Abs. 2 ZAG in Verbindung mit der Delegierten Verordnung (EU) 2018/389 („Del. VO (EU) 2018/389") die Möglichkeit, ausnahmsweise auf die starke Kundenauthentifizierung zu verzichten. Dazu muss einer der in der Del. VO (EU) 2018/389 geregelten Ausnahmefälle einschlägig sein. Zu diesen Ausnahmenfällen zählen unter anderem die Folgenden:

– Wird der Zahlungsempfänger auf einer vom Zahler vor dem Zahlungsvorgang erstellten Liste[12] von vertrauenswürdigen Empfängern geführt, kann die starke Kundenauthentifizierung entfallen, sofern die allgemeinen Anforderungen an die Authentifizierung erfüllt sind.

– Lösen juristische Personen elektronische Zahlungsvorgänge über dezidierte, mithin eigens hierfür eingerichtete Zahlungsprozesse oder -protokolle aus, die nur Zahlern zur Verfügung stehen, die nicht als Verbraucher handeln, kann ebenfalls auf eine starke Kundenauthentifizierung verzichtet werden. Voraussetzung ist aber, dass diese Prozesse oder Protokolle nach Ansicht der Behörden mindestens ein vergleichbares Sicherheitsniveau wie das von der EU-Richtlinie PSD2 [13] beschriebene aufweisen.

– Löst der Zahler an einem unbeaufsichtigten Terminal einen elektronischen Zahlungsvorgang aus, um ein Verkehrsnutzungsentgelt oder eine Parkgebühr zu bezahlen, kann ebenfalls auf die starke Kundenauthentifizierung verzichtet werden.

Insbesondere die erstgenannte Ausnahme stellt in Bezug auf Invisible Payments eine Möglichkeit dar, auf eine starke Kundenauthentifizierung zu verzichten. Dazu müsste dann ein Zahlungsauslösedienst eingesetzt werden, der die Zahlungsaufträge der Kunden an deren Zahlungsdienstleister weiterleitet. Dabei muss sichergestellt sein, dass der Kunde mithilfe technischer Mittel eindeutig identifiziert werden kann, um diesem die jeweiligen Zahlungsaufträge zuordnen zu können.

Rechtliche Voraussetzungen sind gegeben

Um Invisible Payments erfolgreich einsetzen zu können, muss der Supermarkt eine Vielzahl von personenbezogenen Daten im Sinne von Art. 4 Nr. 1 DSGVO erheben und verarbeiten. Es werden beispielsweise der Name des Kunden, die Zahlungsinformationen von dessen Kreditkarte, Foto- und Videoaufnahmen, Informationen zur Identifizierung sowie Logfiles erhoben und verarbeitet.[14]

Die Verarbeitung der Kundendaten erfolgt beim Modell der Invisible Payments im Supermarkt vor allem dadurch, dass der Kunde durch die technischen Systeme automatisch identifiziert wird und die von ihm ausgewählten Produkte erfasst werden. Aus rechtlicher Sicht werden die Erhebung und Verarbeitung der oben genannten Daten zumeist zur Erfüllung des zwischen dem Kunden und dem Supermarkt geschlossenen Kaufvertrages erforderlich sein. Demnach ist die Verarbeitung dieser Daten gemäß Art. 6 Abs. 1 lit. b) DSGVO rechtmäßig, sofern tatsächlich nur solche Daten erhoben werden, die zur Erfüllung des Kaufvertrages erforderlich sind.

Bei der Verarbeitung der personenbezogenen Daten des Kunden muss der Supermarkt auch die Grundsätze des Art. 5 DSGVO beachten. Eine Verletzung der Grundsätze führt zur Rechtswidrigkeit der Datenverarbeitung.

Erfolgt die Erhebung und Verarbeitung von personenbezogenen Daten über das zur Vertragserfüllung erforderliche Maß hinaus, zum Beispiel zur Analyse des Einkaufsverhaltens, muss zur Rechtmäßigkeit der Datenerhebung entweder die Einwilligung des Kunden gemäß Art. 6 Abs. 1 lit. a) DSGVO vorliegen oder der Supermarkt muss gemäß Art. 6 Abs. 1 lit. f) DSGVO ein berechtigtes Interesse an der Erhebung und Verarbeitung der Daten haben.

Zusammenfassend lässt sich festhalten: Aus rechtlicher Sicht sind in Deutschland die Voraussetzungen gegeben, um das Modell der Invisible Payments umzusetzen. Die potenziellen Nutzer sollten dabei ihr Augenmerk vor allem auf die Ausgestaltung der Vereinbarungen zwischen den beteiligten Parteien legen, um eine rechtssichere Abwicklung der Zahlungen zu gewährleisten. Ferner gilt es, die Vorschriften der DSGVO zu beachten. Dann steht den Invisible Payments zukünftig ein breites Anwendungsgebiet offen.

Fußnoten

1) Handelsblatt/Deutsche Presse-Agentur GmbH: Erster Amazon-Supermarkt ohne Kassen öffnet in Seattle (vom 22.01.2018), URL: https://app.handelsblatt.com/unternehmen/handel-dienstleister/amazon-go-erster-amazon-supermarkt- ohne-kassen-oeffnet-in-seattle/20871836.html ?ticket=ST-3282858-jd0hOGGvXAkNRJJhVwPb-ap6 [25.02.2022].

2) Kolbrück, Olaf: So funktioniert Amazon Go: Die Technik hinter dem Zauberwort „Sensor Fusion" (vom 06.12.2016), URL: https://etailment.de/news/stories/Technologie-So-funktioniert- Amazon-Go-Die-Technik-hinter-dem-Zauberwort-Sensor-Fusion-20194 [25.02.2022].

3) Hierzu in Bezug auf Proximity Payments Brandenburg/Leuthner, ZD 2015, 111, 112.

4) Schimansky/Bunte/Lwowski BankR-HdB/Haug, 5. Aufl. 2017, § 51 Rn. 40.

5) BGH, Urt. v. 20.07.2010 - XI ZR 236/07, Rn. 25.

6) Vgl. instruktiv Schur/Schur, JA 2017, 739, 740.

7) Vgl. Schur/Schur, JA 2017, 739, 740.

8) Vgl. Schur/Schur, JA 2017, 739, 740.

9) Vgl. MüKoBGB/Casper, 8. Aufl. 2020, § 675f BGB Rn. 121.

10) Vgl. Schur/Schur, JA 2017, 739, 740.

11) BaFin Journal Mai 2019, S. 6, URL: https://www.bafin.de/SharedDocs/Downloads/DE/BaFinJournal/2019/bj_1905.html [25.02.2022].

12) Die Liste muss vom Kunden erstellt werden und die vertrauenswürdigen Empfänger dürfen auch nicht vom Zahlungsdienstleister vorgeschlagen werden, vgl. Question ID: 2018_4128 aus dem Single Rulebook Q&A der European Banking Authority.

13) Richtlinie (EU) 2015/2366.

14) Examples of Information Collected when using Amazon Services, among others "Just Walk Out", URL: https://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId= 468496&ref_=footer_privacy#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_87C837F9CCD-84769B4AE2BEB14AF4F01 [25.04.2020].