BRANDI
RECHTSANWÄLTE

DATENSCHUTZ IM ONLINEHANDEL

English version

Einleitung

Der Onlinehandel bietet Unternehmen die Möglichkeit, ihre Produkte und Dienstleistungen einer Vielzahl von (potentiellen) Kunden anzubieten und ihre räumliche Reichweite zu vergrößern. Bei dem Besuch von Onlineshops und dem Tätigen von Online-Bestellungen werden personenbezogene Daten durch die Unternehmen verarbeitet. Die Verantwortlichen haben insofern die Vorgaben des Datenschutzrechts, insbesondere der Datenschutz-Grundverordnung (DSGVO), zu beachten. Der vorliegende Beitrag enthält Informationen zum Datenschutz im Onlinehandel und praktische Umsetzungshinweise.

Zum datenschutzkonformen Onlinehandel mittels Gastzugang hat auch die Datenschutzkonferenz (DSK), das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, am 24.03.2022 Hinweise veröffentlicht, die als Orientierungshilfe zu diesem Thema herangezogen werden können.

Rechtsgrundlagen für Datenverarbeitungen bei Bestellungen

Bestellformulare und -portale in Onlineshops ermöglichen es Kunden, online Verträge mit dem Anbieter des Onlineshops zu schließen. Für die dabei stattfindende Verarbeitung von personenbezogenen Daten ist das Vorliegen einer Rechtsgrundlage erforderlich.

Rechtsgrundlage für einzelne Bestellungen und Gastzugänge

Als Rechtsgrundlage für Datenverarbeitungen im Rahmen von Gastzugängen und einzelnen Bestellungen kommt die Vertragserfüllung gem. Art. 6 Abs. 1 S. 1 lit. b) DSGVO in Betracht. Danach ist eine Verarbeitung personenbezogener Daten rechtmäßig, wenn sie für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist.

Nach der Vorschrift ist nur die Verarbeitung der personenbezogenen Daten zulässig, die für die Erfüllung eines einzelnen Vertrages erforderlich sind. Dies gilt insbesondere auch unter Berücksichtigung des Grundsatzes der Datenminimierung gem. Art. 5 Abs. 1 lit. c) DSGVO, wonach die Datenverarbeitung auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein muss. Bei einer erstmaligen Bestellung kann der Verantwortliche nicht per se unterstellen, dass der Kunde zukünftig weitere Bestellungen tätigen wird und die Kundendaten für mögliche, aber ungewisse zukünftige Geschäfte auf Vorrat gespeichert werden sollen. Die Rechtsgrundlage ist demnach nur für die Daten gegeben, die für die Abwicklung der einzelnen Bestellung benötigt werden, nicht jedoch für die Verarbeitung weiterer Daten, etwa im Rahmen eines fortlaufenden Kundenkontos.

Für die Einrichtung eines solchen fortlaufenden Kundenkontos wäre über die zur Vertragserfüllung benötigten Daten hinaus die Verarbeitung weiterer Daten, beispielsweise Registrierungsdaten für die erneute Nutzung des Onlineshops, erforderlich. Damit Kunden bei Bestellungen nicht gezwungen sind, mehr als die für die einmalige Vertragsabwicklung erforderlichen Daten anzugeben und eine dauerhafte Geschäftsbeziehung einzugehen, ist regelmäßig die Bestellung über einen Gastzugang zu ermöglichen, über den nur die zur Durchführung des Vertrages und zur Erfüllung gesetzlicher Pflichten erforderlichen personenbezogenen Daten der Kunden erfasst werden. Mithilfe eines solchen Gastzugangs können Kunden ein Online-Geschäft tätigen, ohne hierfür ein fortlaufendes Kundenkonto anlegen zu müssen.

Verantwortliche, die Waren oder Dienstleistungen im Onlinehandel anbieten, müssen ihren Kunden deshalb immer die Möglichkeit geben, eine Bestellung unabhängig von der Registrierung für ein Kundenkonto vorzunehmen. Es ist damit aber keine Aussage darüber getroffen, ob der Verantwortliche für interne Zwecke alle Bestellungen eines Kundenkontos in einem internen Kundenkonto zusammenfasst.

Rechtsgrundlage für fortlaufende Kundenkonten

Die Datenverarbeitung im Rahmen der Einrichtung und Nutzung eines fortlaufenden Kundenkontos kann aus den vorgenannten Gründen in der Regel nicht mit der Vertragserfüllung gerechtfertigt werden. Hierfür ist eine andere Rechtsgrundlage erforderlich, nämlich die Einwilligung des Betroffenen gem. Art. 6 Abs. 1 lit. a) DSGVO. Mit seiner Einwilligung gibt der Kunde eine entsprechende bewusste Willenserklärung ab, nach der er eine dauerhafte Geschäftsbeziehung eingehen möchte und auch die Verarbeitung von nicht zur Geschäftsabwicklung benötigten Daten erlaubt. Entsprechende Einwilligungen können bereits im Rahmen des Registrierungsprozesses für das Kundenkonto oder direkt im Rahmen der Online-Bestellung eingeholt werden.

Das fortlaufende Kundenkonto wird dann unter Vergabe von Zugangsdaten eingerichtet, damit sich die Kunden gegenüber dem Verantwortlichen eindeutig identifizieren können. Die Kunden haben hierdurch die Möglichkeit, jederzeit auf ihr Konto zuzugreifen und ihre Daten selbst zu ändern oder Bestellungen einzusehen. Durch die dauerhafte Speicherung der Daten können die Kunden künftige Bestellungen ohne die nochmalige Eingabe aller personenbezogenen Daten tätigen.

Die Erteilung der entsprechenden Einwilligung in die Datenverarbeitung bei der Errichtung und Nutzung des fortlaufenden Kundenkon-

tos muss freiwillig geschehen (Art. 4 Nr. 11 und Art. 7 Abs. 4 DSGVO). Es ist daher nicht möglich, die Erfüllung eines Vertrags von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig zu machen, die für die Erfüllung des Vertrags nicht erforderlich sind. Eine Online-Bestellung darf somit grundsätzlich nicht davon abhängig gemacht werden, dass der Kunde zugleich seine Einwilligung für die Erstellung eines Kundenkontos erklärt. Die Kunden im Onlineshop müssen daher bei demselben Verantwortlichen die gleichen Angebote auch auf anderem gleichwertigen Wege als über ein fortlaufendes Kundenkonto bestellen können (vgl. Rn. 37 f. der Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 des Europäischen Datenschutzausschusses (EDSA) vom 04.05.2020). Gleichwertig ist eine Bestellmöglichkeit nach Auffassung der DSK, wenn keinerlei Nachteile entstehen, also Bestellaufwand und -zugang zu diesen Möglichkeiten denen eines laufenden Kundenkontos entsprechen – wie beispielsweise bei einem Gastzugang – und technische und organisatorische Maßnahmen getroffen werden, die ein angemessenes Datenschutzniveau gewährleisten. Ohne einen alternativen Gastzugang oder eine gleichwertige Bestellmöglichkeit kann somit die Freiwilligkeit einer Einwilligung in die Datenverarbeitung im Rahmen eines fortlaufenden Kundenkontos nicht gewährleistet werden. Bei richtiger Interpretation steht es der Gleichwertigkeit dagegen nicht entgegen, wenn die Angebote zwar auch als Gast bestellt werden können, hierbei dann aber möglicherweise besondere Vergünstigungen (Rabatte) nicht genutzt werden können.

In Einzelfällen können besondere Umstände vorliegen, unter denen ein fortlaufendes Kundenkonto ausnahmsweise als für die Vertragserfüllung erforderlich angesehen werden kann. In diesen Ausnahmefällen ist keine Einwilligung in die Datenverarbeitung erforderlich, sondern die Vertragserfüllung gemäß Art. 6 Abs. 1 S. 1 lit. b) DSGVO kann als Rechtsgrundlage herangezogen werden. Nach Auffassung der DSK ist dann dem Grundsatz der Datenminimierung Rechnung zu tragen, indem beispielsweise das Kundenkonto bei Inaktivität automatisiert nach einer kurzen Frist gelöscht wird.

Ein Kundenclub kann sich von einem fortlaufenden Kundenkonto dadurch unterscheiden, dass er nicht oder nicht nur der Erleichterung von künftigen Bestellungen dient, sondern den Kunden etwa den Zugang zu bestimmten Informationen und Funktionen sowie besonderen Angeboten und Aktionen ermöglicht. Soweit die Einrichtung einer Mitgliedschaft in einem Kundenclub gerade Gegenstand eines Vertrages ist, kann insofern also ebenfalls die Vertragserfüllung als Rechtsgrundlage für die damit einhergehende Datenverarbeitung in Betracht kommen.

Rechtsgrundlagen für weitere Datenverarbeitungen im Onlinehandel

Personenbezogene Daten unterliegen dem Grundsatz der Zweckbindung gem. Art. 5 Abs. 1 lit. b) DSGVO. Sie dürfen danach nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

Für den festgelegten Zweck der Bestellabwicklung erhobene personenbezogene Daten dürfen demnach grundsätzlich nicht auch für andere Zwecke, beispielsweise zu Werbezwecken, verarbeitet werden. Vielmehr ist hierfür gegebenenfalls eine gesonderte Rechtsgrundlage erforderlich.

Datenverarbeitung für Werbezwecke

Als Rechtsgrundlagen für Datenverarbeitungen zum Zwecke der Direktwerbung kommen grundsätzlich sowohl die Einwilligung der betroffenen Person gemäß Art. 6 Abs. 1 S. 1 lit. a) DSGVO als auch eine Interessenabwägung gemäß Art. 6 Abs. 1 S. 1 lit. f) DSGVO in Betracht. Ob sich ein Unternehmen für eine Datenverarbeitung zum Zwecke der Direktwerbung auf seine berechtigten Interessen stützen kann oder ob es hierfür eine Einwilligung der betroffenen Person einholen muss, ist in der Regel von einer Einzelfallprüfung abhängig. Bei der Beurteilung, unter welchen Voraussetzungen Direktwerbung in ihren verschiedenen Formen zulässig ist, sind auch die Wertungen aus dem Gesetz gegen den unlauteren Wettbewerb (UWG) zu berücksichtigen. Wettbewerbsrechtlich ist vor allem durch § 7 UWG geregelt, unter welchen Voraussetzungen eine unzulässige unzumutbare Belästigung durch Werbung anzunehmen ist.

Wenn in einem fortlaufenden Kundenkonto die personenbezogenen Daten für Werbezwecke verarbeitet werden, handelt es sich um eine Verarbeitung, die über die bloße Einrichtung und Führung des Kundenkontos hinausgeht. Die Datenverarbeitung ist damit nicht bereits durch die Einwilligung zur Einrichtung und Führung des fortlaufenden Kundenkontos abgedeckt. Erforderliche Einwilligungen der Betroffenen sind insofern gesondert einzuholen. Dies kann ebenfalls bereits im Rahmen des Registrierungs- oder Bestellprozesses oder über die Einstellungen in dem Kundenkonto erfolgen. Wichtig für die praktische Umsetzung ist, dass die Betroffenen aktiv in die Datenverarbeitung einwilligen müssen, indem sie beispielsweise eine Checkbox selbst ankreuzen. Die Einwilligung ist außerdem mit Wirkung für die Zukunft widerruflich, sodass die Kunden die Möglichkeit haben müssen, ihre Einwilligung jederzeit – beispielsweise wiederum über die Kontoeinstellungen – zurückzunehmen. Zu bedenken ist aber insoweit, dass für Bestandskunden gem. § 7 Abs. 3 UWG ohnehin nicht für alle Werbemaßnahmen eine Einwilligung erforderlich ist, sondern teilweise auch eine Widerspruchsmöglichkeit ausreichend sein kann.

Speicherung von Informationen über Zahlungsmittel

Die Speicherung von Informationen über Zahlungsmittel im Rahmen eines fortlaufenden Online-Kundenkontos bedarf nach Ansicht der DSK ebenfalls einer informierten Einwilligung. Der EDSA führt in seinen Empfehlungen 02/2021 zur Rechtsgrundlage für die Speicherung von Kreditkartendaten ausschließlich zum Zweck der Erleichterung weiterer Online-Transaktionen vom 19.05.2021 hierzu aus, dass die Speicherung von Kreditkartendaten nach der Bezahlung von Waren oder Dienstleistungen als solche für die Erfüllung eines Vertrags nicht erforderlich ist, sondern lediglich nützlich, um eine potenzielle nächste Transaktion und den Verkauf zu erleichtern.

Nach den Ausführungen des EDSA seien Finanzdaten als vertrauliche personenbezogene Daten einzustufen, deren Verletzung mit ernsthaften Konsequenzen für den Alltag des Betroffenen einhergehe und deren Verarbeitung zur Erleichterung weiterer Käufe daher ein zunehmendes Risiko von Verstößen gegen die Kreditkartendatensicherheit berge, da sie die Verarbeitung in anderen Systemen impliziere. Aus dem Grund hätten in diesem spezifischen Kontext nach Ansicht des EDSA bei einer Interessenabwägung regelmäßig die Grundrechte und Grundfreiheiten des Betroffenen Vorrang vor dem Interesse des Verantwortlichen. Die Einwilligung gemäß Art. 6 Abs. 1 S. 1 lit. a) DSGVO sei damit die einzige geeignete Rechtsgrundlage für die Rechtmäßigkeit dieser Datenverarbeitung. Um den Sicherheitsrisiken zu begegnen, der betroffenen Person die Möglichkeit zu geben, die Kontrolle über ihre Daten zu behalten und aktiv über die Verwendung ihrer Kreditkartendaten zu entscheiden, sollte daher die ausdrückliche Einwilligung der betroffenen Person eingeholt werden, bevor ihre Kreditkartendaten nach einem Kauf gespeichert werden. Hierfür reicht es beispielsweise aus, direkt bei Angabe der Zahlungsdaten abzufragen, ob die Angaben für die nächste Bestellung gespeichert werden sollen.

Informationspflichten

Nach dem Grundsatz der Transparenz müssen personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Art. 5 Abs. 1 lit. a) DSGVO). Über die im Rahmen des Onlinehandels stattfindenden Datenverarbeitungen sind die Betroffenen daher entsprechend der Informationspflichten aus Art. 13 und 14 DSGVO aufzuklären. Die Informationspflicht umfasst nicht nur die Datenverarbeitung im Rahmen der Abwicklung von Bestellungen, sondern beispielsweise auch Informationen hinsichtlich der Datenverarbeitung bei der Einrichtung und Nutzung eines Gastzugangs oder eines fortlaufenden Kundenkontos, hinsichtlich des Trackings von Nutzern, zum Beispiel mit Hilfe von Cookies und ähnlichen Technologien, hinsichtlich der Datenverarbeitung für Werbezwecke sowie der Speicherung von Informationen über Zahlungsmittel.

In praktischer Hinsicht können die Informationen zum Beispiel über die Datenschutzerklärung auf der jeweiligen Internetseite zur Verfügung gestellt werden. Bei der Gestaltung der Datenschutzerklärung ist auf eine verständliche Sprache und Übersichtlichkeit zu achten. Die Informationspflichten des Art. 13 DSGVO sollten bei erstmaliger Datenerhebung erfüllt werden. Insofern bietet es sich etwa an, in den Bestell- und Registrierungsprozessen bereits auf die Datenschutzerklärung zu verweisen, bevor die Betroffenen den jeweiligen Prozess abschließen.

Technische und organisatorische Maßnahmen

Die im Rahmen des Onlinehandels verarbeiteten personenbezogenen Daten müssen ausreichend geschützt werden. Verantwortliche und Auftragsverarbeiter müssen deshalb geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau für die Daten zu gewährleisten. Hierbei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen (Art. 32 Abs. 1 DSGVO).

Die DSGVO gibt diesbezüglich nicht vor, welche Maßnahmen konkret für welche Online-Funktionen ergriffen werden müssen. Mögliche Maßnahmen sind beispielsweise die Pseudonymisierung und Verschlüsselung von personenbezogenen Daten.

Löschung von Daten

Nach dem Grundsatz der Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. e) DSGVO müssen personenbezogene Daten grundsätzlich in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Die Speicherfrist für personenbezogene Daten sollte demnach auf das unbedingt erforderliche Mindestmaß beschränkt sein.

Um dies praktisch umzusetzen, sollte der Verantwortliche Fristen für die Datenlöschung vorsehen. Insbesondere im Hinblick auf getätigte Bestellungen können gesetzliche Aufbewahrungsfristen bestehen, die den Verantwortlichen dazu verpflichten, die entsprechenden Bestelldaten für eine gewisse Zeit aufzubewahren. Soweit die Speicherung der Daten zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, ist eine umgehende Löschung von Bestelldaten daher nicht möglich. Entsprechende Pflichten zur Aufbewahrung können sich vor allem aus handelsrechtlichen und steuerrechtlichen Vorgaben, insbesondere aus § 257 Handelsgesetzbuch (HGB) und § 147 Abgabenordnung (AO), ergeben.

Beispielsweise bei einem Gastzugang gilt damit grundsätzlich, dass nach Vertragserfüllung nicht mehr benötigte Daten gemäß Art. 17 Abs. 1 lit. a) DSGVO unverzüglich gelöscht werden müssen. Werden die Daten im Übrigen nur noch zur Erfüllung gesetzlich geregelter Aufbewahrungspflichten verarbeitet, sind nach Empfehlung der DSK technische und organisatorische Maßnahmen der Datensperrung zu ergreifen, um diese Daten von den Daten im operativen Zugriff zu trennen.

Fazit

Der Grundsatz der Datenminimierung, nach dem die Datenverarbeitung auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein muss, gilt auch im Onlinehandel. Ohne die entsprechende Einwilligung der betroffenen Person dürfen daher bei Online-Bestellungen regelmäßig nur die personenbezogenen Daten verarbeitet werden, die zur Vertragserfüllung erforderlich sind. Hieraus ergibt sich, dass die Kunden frei entscheiden können müssen, ob sie im Rahmen einer Gastbestellung lediglich einmalig einen Vertrag abschließen beziehungsweise ihre Daten bei jeder Bestellung neu eingeben möchten oder sie eine dauerhafte Geschäftsbeziehung eingehen und sich ein fortlaufendes Kundenkonto einrichten lassen möchten. Verantwortliche, die Waren oder Dienstleistungen im Onlinehandel anbieten, haben ihren Kunden deshalb unabhängig davon, ob sie ihnen daneben ein fortlaufendes Kundenkonto zur Verfügung stellen, grundsätzlich auch einen Gastzugang bereitzustellen.

Es sind außerdem die allgemeinen datenschutzrechtlichen Vorgaben zu berücksichtigen, unter anderem die datenschutzrechtlichen Informationspflichten, die Datensicherheit und der Grundsatz der Speicherbegrenzung.

Johanna Schmale

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Johanna Schmale
Wissenschaftliche Mitarbeiterin

T +49 521 96535 - 890
F +49 521 96535 - 113
M johanna.schmale@brandi.net