Sorgfältiger Umgang mit Kundendaten und Privatsphäre: ein absolutes Muss für den Finanzsektor

Foto: Piwik PRO

Digitale Bezahlsystem-Anbieter wissen längst: digitale Geschäftsmodelle sind erst dann lukrativ, wenn etwa Online-Shops Kundinnen und Kunden möglichst viele Bezahlarten anbieten, die schnelle, sichere und datenschutzkonforme Transaktionen gewährleisten. Denn: Jede Bezahlart repräsentiert aus der Sicht von Händlern und Shops nichts anderes als einen digitalen Touchpoint, den Kundinnen und Kunden nach Möglichkeit ansteuern und mit einer positiven Erfahrung in Verbindung bringen. Die datenbasierte Erfassung dieses Verhaltens erfolgt über spezifische Analytics-Plattformen, der Verbraucherinnen und Verbraucher zustimmen müssen. Tun sie dies, lassen sich daraus positive, wie negative Rückschlüsse auf individuelle Nutzerpräferenzen bei der Anwendung bestimmter Bezahlmethoden ziehen, die dann mit maßgeschneidert ausgespieltem Content zur Conversion, also zum Kauf bzw. Konsum eines Bank-Produktes führen. Aber: Kundendaten werden gerade im Payment-Sektor als hochsensibel erachtet. So gilt auch für Payment Provider in Deutschland das Bankgeheimnis. Die Anforderungen an die Erhebung personenbezogener Daten sind aus diesem Grund auch in diesem Bereich sehr hoch.

Auch Verbraucherinnen und Verbraucher legen mittlerweile einen großen Wert auf den sorgfältigen Umgang mit ihren persönlichen Daten. Deshalb ist es aus unternehmerischer Sicht klug, die Datenschutzbedürfnisse der Menschen zu respektieren und notwendige Maßnahmen zu ergreifen. Das schafft gerade im Hinblick auf die sensiblen Post-Login-Bereiche der Payment Provider ein hohes Maß an Vertrauen, von dem diese selbst, aber auch die Shops, welche die Payment Provider nutzen, profitieren. Aus gutem Grund: Immer mehr Menschen erledigen Transaktionen über mobile Payment Apps, die an Shops angedockt sind.

Für die eingesetzten Analytics-Lösungen ergeben sich vor diesem Hintergrund komplexe Anforderungen. Dabei sollte die datenbasierte Erfassung des Nutzerverhaltens entlang der Customer Journey mindestens folgende fünf Aspekte berücksichtigen:

1. Sicherheit

Shops, die Payment Provider einsetzen, die gleichzeitig Daten mit Hilfe von Analyseverfahren sammeln und verarbeiten, müssen sicherstellen, dass die von ihnen dazu eingesetzte Analytics-Software absolute Sicherheit und volle Kontrolle über die erhobenen Nutzerdaten bietet. Dazu muss die Software vor allem folgende Anforderungen erfüllen:

- Regelmäßige Software-Audits zur Überprüfung der internen Prozesse,
- Beschränkung des Datenzugriffs durch dezidiertes Rollen und Rechtesystem, das einen granularen Zugriff vorsieht (Single-Sign-On, Zwei-Faktor-Authentifizierung),
- Firewalls zum Schutz vor Zugriff durch externe Netzwerke,
- ausreichend redundante Datensicherungsrichtlinien sowie
- sichere HTTPS-Verbindung für alle Datenzugriffe.

Diese Vorkehrungen tragen dazu bei, das Risiko im Falle von Datenlecks zu minimieren, böswillige Cyberattacken zu verhindern und Daten zu schützen.

2. Ort der Datenerhebung und -speicherung

Payment Provider verarbeiten personenbezogene Daten. Shops müssen sich aus diesem Grund davon überzeugen, dass sie die jeweils lokalen Datenschutzgesetze kennen. Dazu gehören sowohl die Gesetze der Länder, in denen die Daten erhoben werden, als auch die Gesetze jener Länder, in denen Daten gespeichert werden.

Deutschland schreibt zum Beispiel vor, dass personenbezogene Daten der Einwohner innerhalb der Landesgrenzen aufzubewahren sind. Bei Nichteinhaltung drohen hohe Geldstrafen. Für Payment Provider, die etwa Daten von in der EU ansässigen Personen sammeln und verarbeiten, empfiehlt es sich, diese auch auf Servern innerhalb der EU zu speichern.

Angesichts der sich in jüngster Vergangenheit in Europa noch einmal verschärften Gesetzeslage, sind etwa Google Analytics oder Adobe Analytics de facto nicht mehr in der Lage, diese spezifischen gesetzlichen Anforderungen zu erfüllen. Bei der Software-Auswahl kommt es insofern auf die On-Premise Option an, die Datenspeicherung auf eigenen Servern am Standort und damit die volle Datenkontrolle ermöglicht. Entscheidend bei der Wahl der Hosting-Option ist es, zu wissen, wo sich der Server bzw. der Standort der Datenerhebung und -speicherung befindet.

3. Datentransfer

Bis vor wenigen Jahren war die Datenübertragung von der EU in die USA im Rahmen des Privacy Shield noch legal. Diese Praxis erforderte keine vorherige Zustimmung. Im Juli 2020 erklärte der Europäische Gerichtshof diese Rechtsgrundlage für unwirksam. Der amerikanische Schutz personenbezogener Daten wurde als unzureichend erachtet. Jede diesbezügliche rechtliche Regelung muss heute zuallererst der EU-Datenschutzgrundverordnung (DSGVO) entsprechen. Um den Verpflichtungen zur Datenübermittlung nachzukommen, müssen Shops bei den eingesetzten Payment Dienstleistern sichergehen, dass dort die volle Datenkontrolle vorliegt. Gerade personenbezogene Daten sollten immer in der EU gespeichert werden.

4. Brancheneinschränkungen

Insbesondere im Payment-Sektor müssen Unternehmen zahlreiche rechtliche Rahmenbedingungen erfüllen. Dazu gehören etwa der Payment Card Industry Data Security Standard (PCIDSS), das SWIFT-Zahlungssystem, der ISO / IEC 27001 Standard oder die EU-Anti-Geldwäsche-Richtlinie.

Analytics-Daten greifen dabei oftmals in den Geltungsbereich oben genannter Gesetze ein. Sammeln Payment Provider etwa Daten wie Browserverlauf, Geräte-IDs, Internet-Protokoll-IP-Adressen, demografische Informationen oder berufliche Positionen, könnten Personen darüber identifiziert werden. Dazu zählen auch persönliche Finanzinformationen wie Passwörter, Steuerinformationen, Bonitätsauskünfte oder Sicherheitsnummern von Kreditkarten. Es handelt sich in diesen Fällen also um personenbezogene Daten. Um Handling-Verstöße gegen diese Art von Daten zu vermeiden, müssen die Shops darauf achten, dass Payment Provider diese Daten angemessen verwalten und sichern.


Foto: Piwik PRO

Maciej Zawadzinski
CEO von Piwik PRO

5. Auf First-Party-Daten fokussieren

Third-Party-Daten werden nach und nach verschwinden. Trotzdem ist es nicht unwahrscheinlich, dass Verhaltensdaten der Nutzer weiterhin geteilt werden (zum Beispiel zwischen Google Analytics und Google Ads). Dies ist gerade für Post-Login Bereiche von Payment Apps hochproblematisch. Mit anderen Worten: Auch sie müssen vor diesem Hintergrund ihre Marketing-Strategie ändern und sich auf datenschutzfreundliche First-Party-Daten fokussieren, die, nach vorheriger Zustimmung, direkt von den Nutzern stammen. Vorteil: Im Vergleich zu Third-Party-Daten zeichnen sich First-Party-Daten durch eine deutlich höhere Präzision aus. Das versetzt gerade auch Payment Provider in die Lage, unmittelbar auf die Customer Journey Einfluss zu nehmen, gleichzeitig aber auch datenschutzfreundlich zu agieren und die Bedürfnisse der Nutzer zu respektieren.

Fazit

Online-Shops suchen fortwährend nach Möglichkeiten neue Kunden zu gewinnen. Dazu gehört auch das Angebot von adäquaten Payment Providern. Technologie unterstützt die Shops dabei, aktuelle und zukünftige Kunden bei der Wahl von Payment Diensten besser zu verstehen und die Customer Journey von Shops zu optimieren. Vor diesem Hintergrund erkennen immer mehr Shops sowohl für den öffentlichen als auch den Post-Login-Bereich den Wert von Web- und Produktanalytik. Sie versetzen sie in die Lage, Kundinnen und Kunden relevante (Payment-) Dienste anzubieten und das Kundenerlebnis zu verbessern.

Allerdings: Branchenvorschriften und Datenschutzgesetze beeinflussen die Wahl einer solchen Technologie. Im Selektionsprozess sollte gerade das Finanzwesen deshalb nicht unbedingt auf prominente Analytics-Lösungen setzen. Es gilt sorgfältig zu überprüfen, ob Lösungen eine gesetzeskonforme Datenerfassung unterstützen, einen angemessenen Schutz der Daten bieten sowie die Privatsphäre des Einzelnen respektieren.