3. Verbraucherdialog „Mobile Payment“

Empfehlungen der Arbeitsgruppe Datenschutz

Mobile Payment ist eine Form des Bezahlens, die in verschiedenen Formen ausgestaltet ist und in unterschiedlichsten Bereichen zum Einsatz kommt. Soweit der Bezahlvorgang kontaktlos erfolgt und hierfür Smartphones eingesetzt werden, ist die Verbreitung in Deutschland noch gering. Die Zahl der Angebote hingegen nimmt stetig zu. Mobile Payment wird das Potential zugesprochen, die Art des Bezahlens erheblich zu verändern. Hierfür muss das Vertrauen der Verbraucherinnen und Verbraucher gewonnen werden. Dies kann nur gelingen, wenn Angebote verbraucherfreundlich ausgestaltet werden und mit den Daten von Verbraucherinnen und Verbrauchern datenschutzfreundlich umgegangen wird.

Eingesetzte Technologien

Anders als bei herkömmlichen Zahlungskarten mit Chip oder Magnetstreifen wird beim Mobile Payment die Bezahlung in elektronischer Form und vor allem kontaktlos bewirkt. Hierbei wird technologisch auf NFC (Near Field Communication), QR(Quick Response)-Code, und andere Technologien gesetzt.

Formen des Mobile Payment

Bei der häufig eingesetzten NFC-Technologie werden drei Formen des Mobile Payment unterschieden:

- Eine **Passive NFC Card** kommuniziert mit einem NFC-Lesegerät, bspw. einem Händlerterminal. Der Bezahlvorgang wird anschließend über öffentliche Kommunikationswege (bspw. das Internet) oder mit Hilfe der Systeme des Zahlungsdienstleisters abgewickelt. Ein typisches Beispiel für eine solche Kommunikation ist das Verwenden kontaktloser Bezahlkarten für das Begleichen von geringen Geldbeträgen.
- Ein **NFC Mobile Device** („Smartphone“) kommuniziert über eine entsprechende Applikation („App“) mit dem NFC-Lesegerät, bspw. einem Händlerterminal. Der Bezahlvorgang wird anschließend über öffentliche Kommunikationswege (bspw. das Internet) oder mit Hilfe der Systeme des Zahlungsdienstleisters abgewickelt. Ein typisches Beispiel für eine solche Kommunikation sind Fahrkarten-Anwendungen für den öffentlichen Personenverkehr.

- Beim Szenario **Passive NFC Card und NFC Mobile Device** kommuniziert eine Passive NFC Card mit einem NFC Mobile Device („Smartphone“), welches als NFC-Lesegerät eingesetzt wird. Der Bezahlvorgang wird anschließend über öffentliche Kommunikationswege (bspw. das Internet) oder mit Hilfe der Systeme des Zahlungsdienstleisters abgewickelt. Typischerweise findet man solche Konfigurationen im Bereich kostengünstig zu realisierender mobiler Händlerterminals.

Datenschutzrechtliche Grundlagen des Mobile Payment

Die datenschutzrechtliche Zulässigkeit privatwirtschaftlicher Datenverarbeitungen bestimmt sich grundsätzlich nach den Regelungen des Bundesdatenschutzgesetzes (BDSG). Dieses tritt allerdings hinter spezielleren Normen zurück, wie sie sich z. B. im Telemediengesetz oder Telekommunikationsgesetz finden. Als ein Bezahlverfahren sind für das Mobile Payment aber auch die Bestimmungen des Bürgerlichen Gesetzbuches, des Gesetzes über die Beaufsichtigung von Zahlungsdiensten oder des Gesetzes über das Kreditwesen von Bedeutung. Mit Blick auf die Zukunft werden auch die Regelungen der geplanten europäischen Datenschutz-Grundverordnung Bedeutung erlangen.

Für Verbraucherinnen und Verbraucher bestehen beim Einsatz von Mobile Payment Angeboten verschiedene **datenschutzrechtliche Risiken**. Diese müssen sowohl bereits **vor Einführung** als auch beim konkreten **Einsatz** von Mobile Payment Angeboten erkannt und so weit wie möglich minimiert werden.

Überlegungen vor Einführung von Mobile Payment Angeboten

Vor der Einführung von Mobile Payment Verfahren ist die **datenschutzrechtliche Relevanz**, also ein möglicher Personenbezug, beispielsweise anhand einer datenschutzrechtlichen Risikobewertung zu prüfen.

Grundlagen des Mobile Payments sind die gesetzliche Erlaubnis (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG), die die Datenverarbeitung nur im Rahmen des Vertragszwecks zulässt, sowie die Einwilligung, soweit die Datenverarbeitung über den Vertragszweck hinausgeht.

Eine ausreichende **Information** versetzt Verbraucherinnen und Verbraucher in die Lage, Vorteile und Risiken des Mobile Payment abzuschätzen und selbstbestimmt über die Anwendung zu entscheiden. Daher müssen sie die Möglichkeit haben, sich schnell und einfach ein Grundwissen über das angebotene Mobile Payment Verfahren anzueignen. Neutrale Grund- und weiterführende Informationen müssen vor der Teilnahme an einem Mobile Payment Verfahren bereitgestellt werden.

Diese Informationen sollten Anbieter den Verbraucherinnen und Verbrauchern vor Vertragsschluss separat überlassen und möglichst auch bei den beteiligten Händlern angeboten werden.

Werden am Ort des Bezahlens Lesegeräte eingesetzt, stellen diese eine weitere Risikoquelle für das informationelle Selbstbestimmungsrecht der Verbraucherinnen und Verbraucher dar. Sie müssen daher als Lesegeräte für das mobile Bezahlen kenntlich gemacht werden. Dabei ist ein möglichst einheitliches Zeichen zu verwenden.

Die Grund- und weiterführenden Informationen über das Mobile Payment sollten mindestens Angaben zu folgenden Punkten in leicht verständlicher Form enthalten:

- Name und Anschrift der Systemanbieter und Händler
- Bezeichnung und Beschreibung der Funktionsweise des Mobile Payment Verfahrens
- Art der verarbeiteten Daten
- Zweck der Datenverarbeitung
- Empfängerkategorien der Daten
- Schlussfolgerungen aus der Risikobewertung mit Grundinformationen zu möglichen Vor- und Nachteilen/Risiken
- Vorschläge für Sicherheitsmaßnahmen
- Beschreibung der Erkennungsmerkmale der Lesegeräte
- Rechte (insb. Auskunfts-, Berichtigungs- und Löschungsrechte)
- Schutzmaßnahmen bei Verlust oder Zerstörung
- Zugriffsrechte bei der Verwendung von Apps: Auf welche Daten wird zugegriffen, an wen werden sie ausgeleitet und ist dies erforderlich?

Persönliche Daten der Verbraucherinnen und Verbraucher dürfen beim Bezahlen nicht ohne deren **Mitwirkung und Kenntnis** ausgelesen werden. Um dies zu gewährleisten, sind die folgenden Punkte zu berücksichtigen:

- Lesegeräte müssen eindeutig erkennbar sein. Dies soll mit einem einheitlichen Zeichen sichergestellt werden.

- Am Lesegerät ist kenntlich zu machen, dass ein Mobile Payment Verfahren eingesetzt wird. Weitere Informationen sind bereit zu halten.

- Lese- bzw. Zahlungsvorgänge sind optisch oder akustisch kenntlich zu machen sowie nachvollziehbar zu gestalten.

- Der Berechtigte ist über das Auslösen eines Zahlungsvorgangs unverzüglich zu informieren (bspw. schriftlich oder durch SMS oder durch E-Mail).

- Die Gewährleistung dieser Anforderungen obliegt Systemanbietern und Händlern innerhalb ihrer Einflussmöglichkeiten.

Folgende **technisch-organisatorischen Maßnahmen** sind zu treffen:

- Für ein verbraucherfreundliches Angebot sollte vor Einführung/Einsatz eines Mobile Payment Verfahrens eine Risikobewertung durchgeführt werden. Durchführung und Ergebnis sind zu dokumentieren und die Schlussfolgerungen daraus Verbraucherinnen und Verbrauchern in verständlicher Form zugänglich zu machen.

- Die möglichen Schutzmechanismen beim Einsatz von Anwendungen auf einem Smartphone sind auszunutzen.
  Voreinstellungen müssen datensparsam ausgestaltet sein, d.h. es muss eine Beschränkung auf die erforderlichen Daten bei Erhebung und Übermittlung erfolgen.
  Es muss für den Schutz vor unberechtigtem Auslesen gesorgt werden.

- Werden Smartphones beim Mobile Payment eingesetzt, dürfen entsprechende Apps nicht vorinstalliert sein oder müssen vor dem Einsatz zumindest eine aktive Freischaltung erfordern. Hierbei müssen die oben beschriebenen Informationen bereitgestellt werden. Die Zugriffsbefugnisse sind auf das erforderliche Maß zu beschränken.

- Schutzmöglichkeiten bei Verlust oder Zerstörung müssen bestehen.

Anforderungen an einen verbraucherfreundlichen Einsatz

Bei der **Anwendung** von Mobile Payment Verfahren müssen die oben dargestellten Überlegungen umgesetzt sein. Darüber hinaus ist Folgendes zu gewährleisten:

- Die Datenverarbeitung muss sich im Rahmen des Vertragszwecks halten oder bedarf einer wirksamen Einwilligung. Hierbei sollte sichergestellt sein, dass eine ausreichende Information erteilt wurde.

- Im Falle der Einwilligung muss diese abgegrenzt von anderen Erklärungen erfolgen und jederzeit einfach mit Wirkung für die Zukunft widerrufen werden können. Wird die Einwilligung elektronisch erteilt, muss dies im Wege des Double-Opt-In-Verfahrens erfolgen und schriftlich bestätigt oder protokolliert und jederzeit abrufbar gehalten werden.

- Die Teilnahme am Bezahlverfahren darf nicht von einer Einwilligung in andere Nutzungszwecke abhängig gemacht werden.

- Die Erhebung der Daten soll soweit möglich direkt und unter aktiver Mitwirkung der Verbraucherinnen und Verbraucher erfolgen.

- Die Teilnahme sollte möglichst anonym möglich sein, soweit dem keine gesetzlichen Regelungen entgegenstehen.

- Die Erhebung von persönlichen Daten ist auf das für den Bezahlvorgang erforderliche Maß zu beschränken.

- Die **erhobenen Daten** sollen nur für die Abwicklung eines sicheren Bezahlvorgangs genutzt werden. Eine Nutzung des Datenmehrwerts soll nicht stattfinden.

- Sobald der Zweck der Datenverarbeitung erreicht ist, eine wirksame Rechtsgrundlage bzw. Einwilligung fehlt oder widerrufen wurde, sind die Daten zu löschen, soweit dem keine sonstigen Aufbewahrungspflichten entgegenstehen. In diesem Fall sind sie zu sperren und weiterhin gegen unberechtigten Zugriff zu schützen.

- Es muss für Verbraucherinnen und Verbraucher einfach sein zu erfahren, welche Daten von ihnen zu welchem Zweck gespeichert sind, woher ihre Daten stammen und wer ihre Daten erhalten hat.

- Verbraucherinnen und Verbraucher müssen ihre Daten einfach berichtigen können.

- Verbraucherinnen und Verbraucher sind über mögliche unberechtigte Datenverarbeitungen unverzüglich zu informieren.

Für die Bank- und Geschäftsprozesse im Hintergrund eines (mobilen) Zahlungsvorgangs sind die regulären Anforderungen an den **technisch-organisatorischen Datenschutz** gemäß § 9 BDSG zu erfüllen. Maßstab hierfür können die Sicherheitsstandards nach dem Stand der Technik gemäß den Vorgaben des BSI sein.

Beim Mobile Payment Verfahren ist aus Verbrauchersicht insbesondere Folgendes zu gewährleisten:

Die Anbieter haben sicherzustellen, dass unbefugte Dritte von der Teilnahme sowie den Daten der Verbraucherinnen und Verbraucher keine Kenntnis nehmen können.

Geeignete Maßnahmen hierzu sind beispielsweise:

- Authentifizierung der teilnehmenden Person (Zwei-Faktor-Authentifizierung)
- lückenlose Verschlüsselung nach aktuellem Stand der Technik bei der Übertragung und Speicherung personenbezogener Daten
- Vorhaltung und Aufbereitung von Protokolldaten in Form und Umfang, so dass Verbraucherinnen und Verbraucher in die Lage versetzt werden, selbständig zu überprüfen, ob Dritte unberechtigt auf ihre Daten zugegriffen haben.

Weiterhin sind folgende Punkte sicherzustellen:

- Nehmen Verbraucherinnen und Verbraucher an mehreren Mobile Payment Verfahren oder Programmen eines Anbieters teil, müssen ihre personenbezogenen Daten getrennt voneinander verarbeitet und gespeichert werden, soweit die Nutzung nicht bloßen Abrechnungszwecken dient.
- Werden mehr Daten erhoben, als für die Durchführung des Zahlungsvorgangs erforderlich sind (z.B. Geo-Lokalisierungen, Sensordaten, etc.), muss hierin im Wege des Opt-In-Verfahrens ausdrücklich eingewilligt werden. Die Erhebung ist dem Nutzer in eindeutiger Form anzuzeigen.
- Der Anbieter ist für die Schließung von Sicherheitslücken verantwortlich und hat die Haftung für die Fehlerfreiheit seines Produktes zu übernehmen.
- Verbraucherinnen und Verbraucher müssen in die Lage versetzt werden, Daten innerhalb ihres Einflussbereichs selbständig und vollständig zu löschen, z.B. durch Deinstallation einer App.

Stand: 04.11.2013