Beschluss der DSK vom 23.03.2018

Kontaktloses Bezahlen

Kontaktloses Bezahlen ist derzeit in vielen Varianten möglich. Der zugrunde liegende Übertragungsstandard Near Field Communication (NFC) wird für Geld- und Kreditkarten sowie für mobiles Bezahlen z.B. mit dem Smartphone genutzt. Die Datenschutzaufsichtsbehörden begleiten die Entwicklung aus datenschutzrechtlicher und –technischer Sicht. So wurde bereits im Beschluss des Düsseldorfer Kreises vom 19. September 2012 zu „Near Field Communication (NFC) bei Geldkarten“ auf die datenschutzrechtlichen Grundanforderungen hingewiesen. Mittlerweile sind die Verantwortlichen vielen dieser Forderungen nachgekommen bzw. mit deren Umsetzung befasst.

Die grundsätzlichen Forderungen bezüglich kontaktloser Bezahlverfahren lassen sich wie folgt zusammenfassen:

Die Notwendigkeit einer Datenschutz-Folgenabschätzung ist nach Artikel 35 DS-GVO zu prüfen.

Die Karten ausgebenden Institute sind verpflichtet, umfassende und verständliche Informationen für Nutzerinnen und Nutzer über Datenhaltung und -verarbeitung bereitzustellen. Bei Bezahlverfahren, die ein Smartphone voraussetzen, ist weiterhin über die damit einhergehenden besonderen Risiken zu informieren. Zudem sind Hinweise zur Risikominimierung zu geben.

Die Kundinnen und Kunden sind darüber zu unterrichten, dass eine kostenlose Schutzhülle in der Standardversion zur Verfügung steht.

Es muss sichergestellt sein, dass durch Voreinstellung die NFC-Funktion zunächst deaktiviert ist. Den Kundinnen und Kunden muss ermöglicht werden, die NFC-Funktion jederzeit abschalten zu können. Alternativ können auch Karten ohne NFC-Funktion angeboten werden, ohne dass für Kundinnen und Kunden Mehrkosten entstehen.

Um das unberechtigte Auslesen etwaiger personenbeziehbarer Daten zu verhindern, ist die drahtlose Kommunikation zwischen (virtueller) Karte und Terminal zu verschlüsseln. Die (Kredit-)Wirtschaft wird aufgefordert, die zurzeit laufenden Arbeiten an einer internationalen Spezifikation der Verschlüsselung weiterhin zu forcieren. Auch bleiben weitere Maßnahmen zur technisch-organisatorischen Absicherung von NFC-basierten Konzepten - wie z.B. die Randomisierung der Kartennummer - fortgesetzt aktuell.

Es sollte grundsätzlich keine Möglichkeit des kontaktlosen Auslesens einer wiederkehrenden Kennziffer (z.B. Kartennummer) möglich sein, die unter Umständen zu Zwecken der Profilbildung herangezogen werden kann.

Bei Bezahlverfahren, die ein Smartphone voraussetzen, ist die Bezahl-App von den ausgebenden Kreditinstituten aktuell zu halten. Die Kundinnen und Kunden sind dazu anzuhalten, nur die aktuellen Software- und Betriebssystemversionen einzusetzen. Bei nicht aktualisierten Software- und Betriebssystemversionen ist mindestens kontinuierlich und unübersehbar darauf hinzuweisen, wenn die Anwendungen zu Sicherheitsrisiken führen.

Die Karten ausgebenden Institute werden darauf hingewiesen, dass etwaige auf der Karte vorhandene Drittanwendungen, die geeignet sind, das Pseudonymisierungskonzept des Bezahlsystems zu unterlaufen, eine neue datenschutzrechtliche Bewertung erforderlich machen. Zudem sind die Drittanbieter darauf hinzuweisen, dass und wie eine mögliche Depseudonymisierung infolge unsachgemäßer Belegung von Datenfeldern zu vermeiden ist.