Verbesserter Schutz von Ausweisdaten

Für die Menschen in Singapur gehörte es lange zum Alltag, bei jeder Gelegenheit die Nummer ihrer Ausweispapiere preisgeben zu müssen – egal, ob es um die Vorbestellung von Kinotickets, die Anmeldung bei einem Onlineportal oder das Betreten eines Gebäudes ging. Mit der Umsetzung einer neuen Richtlinie zum Schutz solcher Ausweisdaten hat diese Praxis nun ein Ende gefunden.

VON SEBASTIAN BLASIUS ::: Am 31. August 2018 erließ die singapurische Datenschutzkommission eine Richtlinie bezüglich der Anwendung des singapurischen Datenschutzgesetzes (Personal Data Protection Act, PDPA) auf nationale Ausweisnummern. Diese Richtlinie bestimmt, dass die Verarbeitung von nationalen Ausweisnummern, also insbesondere deren Erhebung, grundsätzlich untersagt ist. Nur in Ausnahmefällen soll es Organisationen noch erlaubt sein, diese Daten zu verarbeiten.

Am 1. September 2019 begann die Kommission, den PDPA im Sinne der Richtlinie auszulegen. Für Verbraucher sind das gute Nachrichten, denn die Weitergabe sensibler Ausweisdaten an eine unüberschaubare Vielzahl von Dritten birgt etliche Risiken. So wird etwa die Nummer der singapurischen National Registration Identity Card (NRIC), also des Ausweisdokuments singapurischer Staatsangehöriger und Permanent Residents, häufig zur Identitätsverifizierung und Abwicklung von Transaktionen mit singapurischen Regierungsbehörden und Banken genutzt. Gleiches gilt für die Foreign Identification Number (FIN), also die Ausweisnummer, die an in Singapur lebende/arbeitende Ausländer vergeben wird. Geraten diese Nummern in die falschen Hände, kann das schwerwiegende Folgen haben. Unternehmen sollten nun überprüfen, ob ihre Praxis im Umgang mit den genannten Ausweisdaten den Vorgaben der Richtlinie entspricht. Bei Verstößen gegen den PDPA drohen unter anderem Geldbußen von bis zu 1 Mio. Singapur-Dollar.

Dieser Bericht gibt einen kurzen Überblick über den Anwendungsbereich der Richtlinie, die Ausnahmesituationen, in denen es Organisationen weiterhin erlaubt bleibt, Ausweisdaten zu verarbeiten, und die Schritte, die Organisationen ergreifen können, um die Einhaltung der neuen Vorgaben sicherzustellen.

Welche Ausweisdaten erfasst die Richtlinie?

Die Richtlinie erwähnt etwa die FIN sowie die Nummern von NRICs, Reisepässen, Führerscheinen und Geburtsurkunden explizit. Es wird allerdings auch darauf hingewiesen, dass diese Aufzählung nicht abschließend ist. Über die benannten Fälle hinaus gilt die Richtlinie ganz allgemein für die Verarbeitung sämtlicher Arten von nationalen Ausweisnummern (und der zugehörigen Ausweisdokumente).

Ausdrücklich nicht von der Richtlinie erfasst werden unvollständige NRIC-Nummern, wenn diese maximal aus den letzten drei Ziffern und dem die Nummer abschließenden Buchstaben (der sogenannten Checksum) bestehen. Gleiches sollte für andere Identifikationsnummern gelten. Wichtig ist hierbei allerdings der Hinweis, dass auch unvollständige Ausweisnummern im Einzelfall die Identifikation einer Person zulassen können. Dann sind auch diese unvollständigen Nummern als personenbezogene Daten im Sinne des PDPA zu qualifizieren und unterfallen somit dessen allgemeinen Vorschriften.

Bild: Kzenon, Shutterstock

Ausnahmefälle mit großem Auslegungsspielraum

Organisationen dürfen Ausweisdaten nur noch in zwei Ausnahmefällen sammeln und verarbeiten. Zunächst bleibt die Datenverarbeitung erlaubt, wenn eine der Ausnahmevorschriften des PDPA greift oder die Verarbeitung einer Ausweisnummer oder der Kopie eines Ausweisdokuments durch andere Gesetze vorgeschrieben wird. Für Arbeitgeber ist hier insbesondere das singapurische Arbeitsgesetz relevant. Danach sind Arbeitgeber verpflichtet, Arbeitnehmerakten zu führen, die auch die NRIC-Nummer oder FIN des Arbeitnehmers enthalten müssen. Die Verarbeitung dieser Ausweisdaten bleibt also hier erlaubt. Andere alltagsrelevante Fälle sind etwa der Arztbesuch oder das Einchecken in einem Hotel. Ärzte müssen die FIN, NRIC- oder Reisepassnummer einer Person erheben, um sicherzustellen, dass die korrekte Person behandelt wird. Und auch Hotels sind zur Abfrage der Ausweisnummern verpflichtet.

Unternehmen sollten im Einzelfall gut begründen können, warum Ausweisdaten anstelle von weniger sensiblen Informationen abgefragt wurden.

Zudem ist die Verarbeitung von Ausweisdaten auch dann weiterhin möglich, wenn sie notwendig ist, um die Identität einer Person mit einem hohen Maß an Verlässlichkeit festzustellen. Erfasst sind generell Fälle, in denen ohne eine solche Feststellung ein hohes Sicherheitsrisiko oder die Gefahr eines signifikanten Schadens für Personen oder Organisationen bestünde. Zu denken ist diesbezüglich etwa an die Identitätsfeststellung des Besuchers einer Vorschule oder eines Kindergartens. Um die Sicherheit der Kinder zu gewährleisten, ist es hier notwendig, die Identität eines Besuchers zweifelsfrei festzustellen.

Für Unternehmen kann vor allem die Vermeidung eines Schadens im Hinblick auf ihre Finanzen, ihr Eigentum oder ihre Reputation eine verlässliche Identitätsfeststellung erforderlich machen. Häufig wird es dabei um Transaktionen mit Bezug zu Immobilien oder die Geltendmachung von (zum Beispiel Versicherungs-)Forderungen gehen. Letztlich müssen Unternehmen aber selbst eine Bewertung dahingehend vornehmen, ob die Verarbeitung von Ausweisdaten notwendig ist. Die Formulierung der Richtlinie erlaubt erheblichen Auslegungsspielraum. Sollte die Verarbeitung von Ausweisdaten einmal zum Gegenstand einer Kommissionsuntersuchung werden, wird es für die betroffenen Organisationen daher umso wichtiger sein, angemessen und nachvollziehbar belegen zu können, warum die Verarbeitung erforderlich war.

Einbehaltung von Dokumenten

Während die obigen Ausführungen die Verarbeitung von Ausweisnummern und auch das Anfertigen von Kopien von Ausweisdokumenten betreffen, gelten noch strengere Regelungen für Organisationen, die übergebene Ausweisdokumente für eine gewisse Zeit im Original einbehalten möchten. Bisher forderte etwa das Sicherheitspersonal an Gebäudeeingängen häufig die Aushändigung von Ausweisdokumenten im Tausch gegen einen Besucherausweis. Grund für diese Praxis war es in der Regel lediglich, sicherzustellen, dass der Besucherausweis beim Verlassen des Gebäudes wieder zurückgegeben wird. Seit dem 1. September ist diese Vorgehensweise nicht mehr erlaubt. Physische Ausweisdokumente dürfen nun nur noch in Fällen einbehalten werden, in denen dies durch ein Gesetz vorgeschrieben ist.

Was sollten Organisationen nun tun?

Um die Einhaltung der neuen PDPA-Vorgaben sicherzustellen, sollten Organisationen zunächst die eigene Praxis im Umgang mit Ausweisdaten überprüfen und gegebenenfalls anpassen. Häufig wird diesbezüglich auch eine Aktualisierung der unternehmensinternen Datenschutzrichtlinie notwendig sein. Die Erstellung und Implementierung einer solchen Datenschutzrichtlinie ist gesetzlich verpflichtend; und inhaltlich müssen nun dort Fälle abstrakt dokumentiert werden, in denen eine Organisation die Notwendigkeit zur Verarbeitung von Ausweisdaten sieht. Auch im konkreten Einzelfall sollten Unternehmen aber immer belegen können, warum eine Verarbeitung von Ausweisdaten stattfand. Leichter machen es sich Organisationen, wenn sie – sofern möglich – auf die Verarbeitung von Ausweisdaten vollständig verzichten. Oft kann die gewünschte Identifikation einer Person nämlich auch ohne Weiteres durch die Verarbeitung von Daten erreicht werden, die weniger sensibel sind. :::

Sebastian Blasius arbeitet als Rechtsanwalt bei der Luther Rechtsanwaltsgesellschaft in Singapur. Kontakt: sebastian.blasius@luther-lawfirm.com, www.luther-lawfirm.com