Neue Rechte und Pflichten beim Datenschutz

Am 2. November 2020 hat das singapurische Parlament ein Änderungsgesetz zum Personal Data Protection Act (PDPA) erlassen. Ziel ist es, im Bereich des Datenschutzes zeitgemäße und international konkurrenzfähige Marktbedingungen zu schaffen.

VON SEBASTIAN BLASIUS ::: Das Änderungsgesetz wird den bisherigen PDPA in mehreren Phasen reformieren. Die lokale Datenschutzkommission (PDPC) hat diesbezüglich das Schlagwort vom „Enhanced PDPA" eingeführt. Am 1. Februar 2021 traten die ersten Änderungen des PDPA in Kraft. Für singapurische Unternehmen führen sie zu strengeren Pflichten, aber auch zu praktischen Erleichterungen. Viele der Neuerungen werden Unternehmen mit europäischen Wurzeln bekannt vorkommen.

Die jüngsten Reformen des PDPA lassen sich grob in vier Bereiche einteilen. Erstens werden strengere Regelungen im Gebiet der organisatorischen und individuellen Verantwortung für die Einhaltung des PDPA eingeführt. Zweitens werden die Erlaubnistatbestände, auf die Unternehmen ihre Datenverarbeitungsvorgänge stützen können, erweitert. Drittens wird die Autonomie betroffener Personen mit Blick auf ihre personenbezogenen Daten gestärkt. Viertens erhält die PDPC weitergehende Befugnisse, gegen PDPA-Verstöße vorzugehen.

Organisatorische und individuelle Verantwortlichkeit

Die organisatorische Verantwortlichkeit singapurischer Unternehmen – zusammengefasst unter dem Begriff „Accountability Obligation" – fand bisher ihren Ausdruck vor allem in den Pflichten, einen Datenschutzbeauftragten zu benennen sowie eine Datenschutzrichtlinie und ein Beschwerdeverfahren zu implementieren. Orientiert an modernen Datenschutzgesetzen anderer Jurisdiktionen, zum Beispiel an der europäischen Datenschutzgrundverordnung (DSGVO), wurden die genannten Obligationen nun durch eine Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten ergänzt.

Eine relevante „Datenpanne" kann etwa vorliegen, wenn eine Organisation ein Speichermedium (zum Beispiel einen USB-Stick oder eine Festplatte) verliert, auf dem personenbezogene Daten gespeichert sind, oder wenn ein Dritter unbefugt auf personenbezogene Daten im Besitz einer Organisation zugreift. Eine solche Panne ist nach den neuen Regeln meldepflichtig, wenn sie der betroffenen Person einen erheblichen Schaden zufügt (oder zufügen könnte) oder von erheblichem Ausmaß ist (oder sein könnte). Organisationen sind beim Verdacht einer Datenschutzverletzung verpflichtet zu prüfen, ob die genannten Kriterien erfüllt sind. Ist das der Fall, muss die PDPC so schnell wie möglich benachrichtigt werden, spätestens aber drei Kalendertage nach Abschluss der vorgenannten Prüfung. Darüber hinaus besteht, vorbehaltlich bestimmter Ausnahmen, die Pflicht, jede betroffene Person über die Datenverletzung zu informieren. Organisationen sollten vor diesem Hintergrund schnellstmöglich einen „Data Breach Management Plan" implementieren, um auf mögliche und tatsächliche Datenlecks angemessen und rechtzeitig reagieren zu können. Die PDPC hat die Befugnis, die Umstände einer Datenverletzung und die Reaktion einer Organisation darauf zu überprüfen, und kann gegebenenfalls Durchsetzungsmaßnahmen ergreifen.

Auf individueller Ebene führte die PDPA-Reform zusätzliche Straftatbestände ein, um Personen für Gesetzesverletzungen zur Rechenschaft ziehen zu können. Sind gewisse Voraussetzungen erfüllt, so kann etwa die unbefugte Weitergabe oder Verwendung personenbezogener Daten zu Geld- und/oder oder Gefängnisstrafen führen. Gleiches gilt, wenn bei bereits anonymisierten Daten unbefugt Handlungen vorgenommen werden, um eine erneute Identifizierung der betroffenen Person zu erlauben.

Erweiterung der Erlaubnistatbestände

Auch im Bereich der Erlaubnistatbestände, also der Vorschriften, die Unternehmen eine Datenerhebung, -nutzung

Der Stadtstaat Singapur stellt sich in puncto Datenschutz neu auf. Das hat auch für ausländische Unternehmen Konsequenzen.

und -weitergabe erlauben, führen die PDPA-Reformen teilweise zu einer Angleichung an die DSGVO. Das betrifft vor allem Datenverarbeitungsvorgänge, die berechtigten Interessen (zum Beispiel des Unternehmens oder der Allgemeinheit) dienen. Unter der DSGVO war eine solche Datenverarbeitung bereits in der Vergangenheit privilegiert. Im PDPA fehlte hingegen eine entsprechende Regelung. Eine solche wurde nun eingeführt und die Datenverarbeitung ist jetzt – auch ohne Einwilligung der betroffenen Person – erlaubt, wenn berechtigte Interessen jegliche negativen Effekte auf die Person, deren Daten betroffen sind, überwiegen. Eine Datenverarbeitung zu Zwecken der Geschäftsoptimierung ist nun ebenfalls privilegiert und oftmals ohne die Einwilligung der betroffenen Person möglich. Erfasst sind insbesondere Datenverarbeitungsvorgänge, die der Entwicklung oder Verbesserung von Waren/Dienstleistungen oder Prozessen einer Organisation oder der Analyse von Kundenverhalten und -präferenzen dienen.

Neben weiteren zusätzlichen Erlaubnistatbeständen wurden auch zwei neue Formen der fingierten Einwilligung in den PDPA aufgenommen. Die Einwilligung einer betroffenen Person kann nun unter Umständen fingiert werden, wenn sie über die beabsichtigte Datenverarbeitung in angemessener Weise informiert wurde und dieser nicht innerhalb einer gesetzten Frist widersprochen hat. Man spricht hier von einem „deemed consent by notification". Voraussetzung ist, dass die beabsichtigte Datenverarbeitung mit Wahrscheinlichkeit keine nachteiligen Auswirkungen auf die betroffene Person hat. Relevant werden soll dieser Erlaubnistatbestand vor allem, wenn eine Organisation bereits personenbezogene Daten für einen bestimmten Zweck in zulässiger Weise erhoben hat und diese nun für einen Sekundärzweck nutzen oder weitergeben möchte.

Bild: VideoFlow, Shutterstock

Daneben gibt es nun mit dem „deemed consent by contractual necessity" eine fingierte Einwilligung im Bereich der Weitergabe vertragsrelevanter Daten. Stellt eine Person P einer Organisation A im Hinblick auf einen zwischen den beiden zu schließenden Vertrag personenbezogene Daten zur Verfügung, wird die Einwilligung Ps in die Weitergabe der Daten durch A an dritte Organisationen fingiert, wenn sie für den Vertragsschluss zwischen P und A notwendig ist. Haben P und A hingegen bereits einen Vertrag geschlossen, ist die Weitergabe der von P zur Verfügung gestellten Daten durch A an eine dritte Organisation erlaubt, wenn sie für die Durchführung desVertrages zwischen P und A oder für den Abschluss oder die Durchführung eines Vertrages zwischen A und der dritten Organisation notwendig ist. Dies gilt dann, wenn der Vertrag auf Verlangen Ps geschlossen wird oder zumindest objektiv in Ps Interesse ist.

Stärkung der Autonomie betroffener Personen

Vorerst noch nicht umgesetzt wurde die im Änderungsgesetz aus 2020 vorgesehene „Data Portability Obligation", die betroffenen Personen mehr Autonomie und Kontrolle über ihre personenbezogenen Daten gewähren soll. Es geht hier um das Recht einer Person, eine Organisation aufzufordern, personenbezogene Daten, die sich im Besitz oder unter der Kontrolle der Organisation befinden, einer anderen Organisation zur Verfügung zu stellen. Erleichtert werden soll so vor allem der Wechsel zwischen verschiedenen Dienstleistern (zum Beispiel Telekommunikationsdienstleistern). Auch das Recht auf Datenübertragbarkeit ist aus der DSGVO schon in ähnlicher Form bekannt.

Härtere Sanktionen

Bereits vor der PDPA-Reform hatte die PDPC weitreichende Befugnisse, um gegen Unternehmen, die das lokale Datenschutzgesetz nicht befolgten, vorzugehen. Dennoch entsteht auch fast zehn Jahre nach Erlass des PDPA noch häufig der Eindruck, dass Unternehmen die Gesetzestreue in diesem Bereich eher als Kür denn als Pflicht ansehen. Die jetzigen Änderungen könnten ein weiterer Beitrag sein, das zu ändern. Nach vollständiger Umsetzung des Änderungsgesetzes drohen bei Gesetzesverstößen Geldstrafen bis zu einer Million Singapur-Dollar und bei Unternehmen, deren Jahresbruttoumsatz 10 Millionen Singapur-Dollar übersteigt, bis zu 10% dieses Umsatzes.

Die jüngste PDPA-Reform führt zu weitreichenden Änderungen im singapurischen Datenschutzrecht. Zu einem großen Teil findet dabei eine Angleichung an die Vorschriften der DSGVO statt. Die Führungsebenen singapurischer Unternehmen sind gut beraten, sich mit den Änderungen auseinanderzusetzen. Neben verschärften Pflichten, vor allem in Hinblick auf die Meldung von Datenschutzverletzungen, bieten sich auch Chancen, datenschutzrelevante Abläufe zu vereinfachen. :::

Sebastian Blasius ist seit 2015 als Rechtsanwalt in Singapur tätig.
Sebastian.Blasius@GatewayLaw.com; +6589028272
https://gateway-law.com/sebastian-blasius-german/