



Datenschutz, die Zweite!

Während viele singapurische Unternehmen noch mit den Anforderungen ihres nationalen Datenschutzgesetzes zu kämpfen haben, müssen sie sich nun zusätzlich auf die europäische Datenschutz-Grundverordnung vorbereiten. Angesichts der Androhung empfindlicher Sanktionen sollten sich Entscheidungsträger (spätestens) jetzt bewusst machen, ob diese Verordnung für ihren Konzern gilt und welche Anforderungen sie stellt.

VON SEBASTIAN BLASIUŠ :: Rund fünf Jahre ist es her, dass mit dem Personal Data Protection Act (PDPA) in Singapur erstmals ein umfassendes Regime zum Schutz persönlicher Daten eingeführt wurde. Während in der EU ähnliche Regeln schon lange bekannt waren, bedurfte es in dem Stadtstaat umfassender Bemühungen der Datenschutzkommission, um die Vorschriften in das Bewusstsein lokaler Organisationen zu bringen. Die Verstärkung des Datenschutzes ist aus Sicht von Privatpersonen und Arbeitnehmern mehr als begrüßenswert. Für einen beachtlichen Teil der Unternehmen erscheint das Thema allerdings vor allem als administrative und kostenverursachende Bürde. Nicht zuletzt aus diesem Grund wird es häufig schlichtweg ignoriert. Mit der europäischen Datenschutz-Grundverordnung (DSGVO), die am 25. Mai 2018 in Kraft tritt, verschärft sich die Situation noch einmal.

Beschränkte Geltung für singapurische Unternehmen

Die gute Nachricht vorab: Die DSGVO wird für einen beträchtlichen Teil der singapurischen Unternehmen keine

Rolle spielen. Zunächst beansprucht sie für außerhalb der EU ansässige Firmen nämlich nur dann Geltung, wenn es um die Verarbeitung von Daten solcher Personen geht, die sich in der Union aufhalten (unabhängig von deren Staatsangehörigkeit). Auch wenn dies der Fall ist, greift die Verordnung aber nur in zwei Konstellationen.

Zum einen findet die DSGVO Anwendung, wenn die Verarbeitung von Daten offensichtlich dem Zweck dient, einer betroffenen Person in der Europäischen Union (entgeltlich oder unentgeltlich) Waren oder Dienstleistungen anzubieten. Ob diese Voraussetzung bejaht werden kann, wird in der Praxis oft eine schwer zu beurteilende Frage sein. Es ist Aufgabe der Rechtsprechung, hier Konkretisierungen zu definieren. Aus den Erwägungsgründen der DSGVO lässt sich jedenfalls entnehmen, dass die bloße Zugänglichkeit einer Website von der EU aus hierfür nicht ausreicht.

Gleiches gilt für die Verwendung der Sprache eines EU-Mitgliedstaats, wenn diese ebenfalls im Land des außereuropäischen Unternehmens gebräuchlich ist. Diese Bewertung



Nach dem Personal Data Protection Act müssen singapurische Unternehmen einen Datenschutzbeauftragten benennen. Die EU-DSGVO sieht das nicht zwingend für alle Firmen vor.

sollte insbesondere singapurische Firmen aufatmen lassen. Englisch ist im Inselstaat Amts- und Verkehrssprache. Nicht jedes Unternehmen, das seine Website auf Englisch gestaltet, muss also direkt mit dem „Vorwurf“ rechnen, sein Angebot auf Kunden in der EU auszurichten. Anders kann dies wiederum bewertet werden, wenn darüber hinaus auch eine Zahlung in der Währung eines der EU-Mitgliedstaaten oder der Versand in die Union angeboten werden oder wenn ein Unternehmen mit vorherigen EU-Kunden wirbt.

Zum anderen unterliegt die Datenverarbeitung auch dann der DSGVO, wenn sie dem Zweck dient, das innerhalb der Europäischen Union erfolgende Verhalten einer Person zu beobachten. Es geht hierbei vor allem um die Verfolgung von Internetaktivitäten. Das gilt insbesondere in Fällen, in denen dadurch ein Profil einer Person erstellt werden kann, durch das persönliche Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder vorausgesagt werden sollen. Erfasst wird damit vor allem Webtracking durch Cookies oder Social Plug-ins.

Viel Bekanntes, aber auch Neues

Inhaltlich schützt die DSGVO Personen im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten. Das sind Daten, die sich auf einen identifizierten oder identifizierbaren Menschen beziehen. Der Begriff der Datenverarbeitung ist dabei weit gefächert. Erfasst werden vor allem die Erhebung, die Speicherung, die Bearbeitung oder die Weitergabe von Daten. Hier gelten gewisse Spielregeln. Grundsätzlich erfordert eine Datenverarbeitung die Einwilligung der betroffenen Person. Darüber hinaus dürfen personenbezogene Daten nur für festgelegte und legitime Zwecke erhoben und verarbeitet werden, müssen angemessen gesichert und eventuell wieder gelöscht werden. Betroffene haben ein Auskunftsrecht, ein Recht auf Berichtigung und auf Löschung sowie ein Widerspruchsrecht. All das ist in ähnlicher Form bereits aus dem PDPA bekannt. Die besondere Herausforderung für singapurische Unternehmen wird daher darin liegen, zu analysieren, inwiefern die DSGVO Anforderungen stellt, die über die des PDPA hinausgehen.

Hinzu kommen aber auch einige regulatorische Neuheiten. Dazu gehört etwa das Recht, keiner rechtlichen Wirkung entfaltenden Entscheidung unterworfen zu werden,

die ausschließlich auf einer automatisierten Verarbeitung personenbezogener Daten beruht. Außerdem kann für Unternehmen die Pflicht bestehen, eine Abschätzung der Folgen vorgesehener Datenverarbeitungsvorgänge durchzuführen. Eine Verletzung des Schutzes personenbezogener Daten muss unter Umständen sowohl der Aufsichtsbehörde als auch der betroffenen Person gemeldet werden – und zwar unverzüglich.

Umfassende Informationspflichten

Bedeutend größer als beim PDPA ist der Umfang der Informationen, die einer betroffenen Person bei der Erhebung ihrer Daten mitgeteilt werden müssen. Hierzu gehören grundsätzlich nicht nur Informationen über das Unternehmen und die beabsichtigte Datenverarbeitung, sondern gegebenenfalls auch eine Belehrung über das Bestehen bestimmter Rechte der betroffenen Person (zum Beispiel über das Auskunfts-, Widerrufs- oder Beschwerderecht). Für Unternehmen bietet es sich hier an, standardisierte Informationsblätter oder eine an Kunden gerichtete Datenschutzrichtlinie zu entwerfen.

Verarbeitet ein außerhalb der EU ansässiges Unternehmen personenbezogene Daten zu den oben genannten Zwecken, hat es grundsätzlich einen innerhalb der Europäischen Union niedergelassenen Vertreter zu benennen. Dies wird zu administrativen Kosten führen. Ausnahmen können aber greifen, wenn die Datenverarbeitung nur gelegentlich erfolgt und keine besonders sensiblen Daten betroffen sind (also etwa solche über die ethnische Herkunft, politische Anschauungen oder sexuelle Vorlieben). Der Vertreter dient insbesondere Behörden und betroffenen Personen als Anlauf- und Kontaktstelle.

Die Benennung eines Datenschutzbeauftragten, der für die Überwachung und Einhaltung der DSGVO zuständig ist, ist hingegen – anders als nach dem PDPA – nicht für alle Unternehmen zwingend. Die DSGVO beurteilt vielmehr anhand der Kerntätigkeit eines Unternehmens, ob ein Datenschutzbeauftragter zu benennen ist. Zur Sicherstellung der Einhaltung der DSGVO erscheint eine Benennung aber jedenfalls als sinnvoll.

Horrende Geldbußen

Als neu (und erschreckend) erweisen sich für singapurische Unternehmen die nach der DSGVO möglichen Geldbußen. Während bei Verstößen gegen den PDPA maximal eine Strafe von 1 Mio. Singapur-Dollar (knapp 625.000 Euro) droht, sind bei Verstößen gegen bestimmte Vorschriften der DSGVO Geldbußen von bis zu 20 Mio. Euro oder 4% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres möglich. Das sollte einen Anreiz dafür schaffen, das neue Datenschutzrecht nicht zu ignorieren. ❖

Sebastian Blasius arbeitet als Rechtsanwalt in Singapur.