

SEBASTIAN BLASIUS

Erlaubnistatbestände im singapurischen Datenschutzrecht

Anstehende Reformen und Vergleich mit der DS-GVO

Internationales Datenschutzrecht
Rechtsvergleich
Berechtigte Interessen
Opt-out
Fingierte Einwilligung

■ Die bevorstehenden Reformen im singapurischen Datenschutzrecht erweitern die Erlaubnistatbestände, auf die Organisationen ihre Datenverarbeitungsvorgänge stützen können. Vor allem die Einführung einer fingierten Einwilligung im Bereich der Vertragserfüllung sowie eines allgemeinen Erlaubnistatbestands zur Wahrung berechtigter Interessen führt dabei zu einer Angleichung der Erlaubnistatbestände des Personal Data Protection Act und der DS-GVO. Dieser Beitrag analysiert die relevanten Vorschriften und zieht Parallelen zwischen singapurischem und europäischem Recht. Er zeigt auf, wo sich die beiden Rechtsordnungen annähern, hebt aber auch Unterschiede hervor. Er dient so vor allem als Leitfaden für deutsche Unternehmen, die in Singapur aktiv sind oder es werden möchten.

Lesedauer: 20 Minuten

■ The pending reforms of the Singaporean data protection law lead to a widening of the statutory permissions upon which the organizations can base their data processing procedures. In particular, the introduction of fictitious consent in the area of contractual fulfillment, as well as a general statutory permission to maintain justified interests will thus lead to an alignment of the Personal Data Protection Act and the General Data Protection Regulation (GDPR/DS-GVO). This article will analyze the relevant provisions and will draw parallels between Singaporean and European law. It will demonstrate where the two legal systems are converging but will also show differences. Thus, it will predominantly serve as a guide for German companies who are active in Singapore or would like to become active there.

I. Einführung

Der Personal Data Protection Act 2012¹ (PDPA) wurde im Jahr 2012 vom *singapurischen Parlament* erlassen und trat Anfang 2014 vollständig in Kraft.² Er ist das erste umfassende Gesetz zum Schutz personenbezogener Daten in Singapur und Ausdruck der Motivation, in diesem Bereich zeitgemäße und international konkurrenzfähige Marktbedingungen zu schaffen. Am 2.11.2020 hat das *singapurische Parlament* nach mehrjähriger Öffentlichkeitsbeteiligung ein Änderungsgesetz zum PDPA erlassen: die Personal Data Protection (Amendment) Bill³ (PDPA-ÄG). Das PDPA-ÄG wird das singapurische Datenschutzrecht in grundlegenden Bereichen umgestalten. Die lokale *Personal Data*

Protection Commission (PDPC) erwartet, dass das Gesetz Anfang 2021 in Kraft tritt.⁴

Viele Konzepte, die das PDPA-ÄG erstmals in den PDPA einführen wird, sind offenkundig an modernen Datenschutzgesetzen anderer Jurisdiktionen orientiert. Dazu zählen etwa

- die Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die *PDPC* und an betroffene Personen, Sec. 26A ff. des neuen PDPA (N-PDPA)⁵,
- das Recht auf Datenübertragbarkeit, Sec. 26F ff. N-PDPA⁶,
- sowie die Möglichkeit, bei Gesetzesverstößen die Höhe einer Geldstrafe am Umsatz einer Organisation zu orientieren, Sec. 48J Abs. 3 N-PDPA⁷.

Die praktisch größte Relevanz des PDPA-ÄG wird allerdings in der Erweiterung und Umgestaltung der Voraussetzungen liegen, unter denen eine Erhebung, Nutzung und Weitergabe (zusammen nachfolgend: Verarbeitung) personenbezogener Daten erlaubt ist. Diese Thematik bildet den zentralen Ausgangspunkt eines jeden Datenschutzgesetzes. Insbesondere Mitglieder deutscher Unternehmensgruppen müssen sich bislang da-

¹ Abrufbar unter: <https://sso.agc.gov.sg/Act/PDPA2012#legis>.

² Vgl. o. Fußn. 1.

³ Abrufbar unter: <https://sso.agc.gov.sg/Bills-Supp/37-2020/Published/20201005?DocDate=20201005>.

⁴ *PDPC*-Website, abrufbar unter: <https://www.pdpc.gov.sg/FAQ-Listing?persona=business-owner&topic=enhanced-pdpa>.

⁵ Beruhend auf Sec. 13 PDPA-ÄG.

⁶ Beruhend auf Sec. 14 PDPA-ÄG.

⁷ Beruhend auf Sec. 24 PDPA-ÄG.

mit abfinden, dass einige Vorschriften, auf die die Gruppe unter der DS-GVO ihre Datenverarbeitung stützt, unter dem Regime des PDPA nicht in vergleichbarer Weise existieren. Das betrifft vor allem die Datenverarbeitung zur Wahrung berechtigter Interessen. Das PDPA-ÄG führt im Bereich der Erlaubnistatbestände zu umfassenden Reformen und einer Angleichung der beiden Rechtsordnungen.

Ziel dieser Ausarbeitung ist es, die Erlaubnistatbestände des singapurischen Datenschutzrechts zu analysieren und Parallelen zu den Erlaubnistatbeständen der DS-GVO zu ziehen. Der Fokus liegt dabei auf den durch das PDPA-ÄG neu eingeführten Regelungen. Bereits bestehende Vorschriften werden hingegen nur in groben Zügen adressiert. Eine detaillierte Darstellung der Erlaubnistatbestände (III.) und allgemeine Ausführungen zum PDPA (II.) dienen der Einordnung und Bestimmung der Relevanz der Erlaubnistatbestände.

II. Allgemein

Der PDPA regelt die Verarbeitung von personenbezogenen Daten durch Organisationen, Sec. 3 PDPA. Personenbezogene Daten i.S.d. PDPA sind (wahre oder unwahre) Informationen über eine Person, die die Identifizierung dieser Person ermöglichen. Die Identifizierung muss dabei entweder allein auf Grund der in Rede stehenden Informationen oder auf Grund dieser Informationen und anderen Daten, zu denen eine Organisation tatsächlich oder wahrscheinlich Zugang hat, möglich sein, Sec. 2 Abs. 1 PDPA.

Zuständig für die Administration des PDPA ist die *PDPC*, Sec. 5 Abs. 2 PDPA. Sie ist insbesondere ermächtigt, verbindliche „regulations“⁸ zur Durchführung des PDPA zu erlassen, Sec. 65 PDPA⁹. Darüber hinaus veröffentlicht sie gem. Sec. 49 Abs. 1 PDPA (unverbindliche)¹⁰ „advisory guidelines“, in denen sie ihre Auslegung der Vorschriften des PDPA darlegt,¹¹ und entscheidet sie auf Grund ihrer quasi-gerichtlichen Befugnisse (s. insbesondere Sec. 28 f. PDPA bzw. Sec. 48H ff. N-PDPA¹²) über mögliche PDPA-Verletzungsfälle.¹³

Der PDPA findet lediglich Anwendung auf in Singapur stattfindende Handlungen.¹⁴ Aus der Definition des Begriffs „organisation“ ergibt sich aber, dass das unabhängig davon gilt, ob die handelnde Organisation ein singapurisches oder ein ausländisches Unternehmen ist und ob sie einen Geschäftssitz in Singapur hat oder nicht, Sec. 2 Abs. 1 PDPA. Anders als die DS-GVO in ihrem Art. 3 Abs. 2 enthält der PDPA keine Vorschriften, die eine Anwendung des Gesetzes auf im Ausland stattfindende Handlungen von Organisationen ohne Sitz im Inland ermöglichen.

Die Verarbeitung personenbezogener Daten ist unter dem PDPA nur dann rechtmäßig, wenn sie sich auf einen Erlaubnistatbestand stützen kann, Sec. 13 PDPA. Dieser Grundsatz erfährt allerdings mehrere Einschränkungen, insbesondere die beiden Folgenden:

- Erstens dürfen geschäftliche Kontaktinformationen (business contact information) auch ohne den Rückgriff auf einen Erlaubnistatbestand verarbeitet werden, Sec. 4 Abs. 5 PDPA¹⁵. Der Begriff umfasst den Namen einer Person, ihre Position oder ihren Titel, ihre geschäftliche Telefonnummer/Adresse/E-Mail-Adresse/Faxnummer und ähnliche Informationen, wenn diese zumindest auch für geschäftsbezogene Zwecke bereitgestellt werden, Sec. 2 Abs. 1 PDPA.
- Zweitens profitieren Auftragsverarbeiter, die gem. Sec. 2 Abs. 1 PDPA als „data intermediaries“ bezeichnet werden, von einer Ausnahmeregelung. Verarbeiten „data intermediaries“ auf Grund eines schriftlichen Vertrags für eine andere Organisation personenbezogene Daten, bedürfen sie hierfür keines Erlaubnistatbestands, Sec. 4 Abs. 2 PDPA¹⁶.

III. Die Erlaubnistatbestände des PDPA

1. Einwilligung

a) Tatsächliche Einwilligung

Wie in Art. 6 Abs. 1 lit. a DS-GVO steht auch im PDPA der Erlaubnistatbestand der Einwilligung vor allen anderen Erlaubnistatbeständen. Gem. Sec. 13 lit. a PDPA darf eine Organisation personenbezogene Daten verarbeiten, wenn die betroffene Person ihre Einwilligung in die Verarbeitung für einen bestimmten Zweck tatsächlich erteilt hat. Die Einwilligung kann dabei ausdrücklich oder konkludent erfolgen.¹⁷ Was die Anforderungen an eine wirksame Einwilligung angeht, ist das singapurische Recht weitaus weniger detailliert als das europäische. Hervorgehoben werden soll hier nur, dass gem. Sec. 14 Abs. 1 lit. a., 20 Abs. 1 lit. a und lit. b PDPA für das Vorliegen einer wirksamen Einwilligung grundsätzlich eine vorherige Information über den Zweck der Datenverarbeitung erforderlich ist, die sog. „notification of purpose“.

b) Deemed Consent by Conduct

Existiert keine tatsächliche Einwilligung, erlaubt Sec. 13 lit. a PDPA die Datenverarbeitung auf Grund der Einwilligungsfiktion des „deemed consent by conduct“¹⁸. Eine fingierte Einwilligung in eine Datenverarbeitung zu einem bestimmten Zweck liegt nach dem Wortlaut der Sec. 15 Abs. 1 PDPA vor, wenn eine Person einer Organisation – ohne eine tatsächliche Einwilligung erteilt zu haben – freiwillig ihre personenbezogenen Daten für einen bestimmten Zweck zur Verfügung stellt und das auch angemessen ist.

Die *PDPC* legt den Wortlaut der Vorschrift weit aus. Eine Zurverfügungstellung kann nach ihrer Ansicht auch dann vorliegen, wenn eine Person die Daten zwar nicht selbst zur Verfügung stellt, aber Handlungen unternimmt, die eine Datenerhebung zulassen. Die Grenze wird dann wiederum durch das Kriterium der Freiwilligkeit gesetzt, das jedenfalls eine entsprechende Absicht hinsichtlich der Zurverfügungstellung erfordert. Weiter muss die Zweckbestimmung aus objektiver Sicht offensichtlich sein.¹⁹

Es hängt von den Umständen des Einzelfalls ab, ob eine fingierte Einwilligung auch die Weitergabe erhobener personenbezogener Daten an dritte Organisationen erfasst. Ist das der Fall, ist jedenfalls auch die Datenverarbeitung durch diese dritten Organisationen von der fingierten Einwilligung gedeckt, Sec. 15 Abs. 2 PDPA.

⁸ Eine Liste der erlassenen „regulations“ veröffentlicht die *PDPC* unter: <https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act>.

⁹ Vgl. Sec. 29 PDPA-ÄG zu den bevorstehenden Änderungen in diesem Bereich.

¹⁰ Vgl. auch *Lim*, *Data Protection in the Practical Context*, 2017, S. 37.

¹¹ Eine Liste der bestehenden „advisory guidelines“ veröffentlicht die *PDPC* unter: <https://www.pdpc.gov.sg/Guidelines-and-Consultation?type=advisory-guidelines>.

¹² Beruhend auf Sec. 23 PDPA-ÄG.

¹³ Sämtliche Entscheidungen der *PDPC* sind abrufbar unter: <https://www.pdpc.gov.sg/All-Commissions-Decisions>.

¹⁴ *Greenleaf*, in: *Chesterman*, *Data Protection Law in Singapore*, 2. Aufl. 2018, S. 482.

¹⁵ Sec. 3 PDPA-ÄG ergänzt die Vorschrift, ohne dass das zu einer Änderung im beschriebenen Bereich führt.

¹⁶ Sec. 3 PDPA-ÄG ergänzt die Vorschrift, ohne dass das zu einer Änderung im beschriebenen Bereich führt.

¹⁷ *PDPC*, [2019] SGPDP 8, 5 f., abrufbar unter: <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Grounds-of-Decision---German-European-School-Singapore--030619.pdf?la=en>.

¹⁸ Zum Begriff vgl. *PDPC*, *Draft Advisory Guidelines on Key Provisions of the Personal Data Protection (Amendment) Bill*, Stand: 20.11.2020, S. 5, abrufbar unter: [https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Draft-AG-on-Key-Provisions/Draft-Advisory-Guidelines-on-Key-Provisions-of-the-PDP-\(Amendment\)-Bill-\(20-Nov-2020\).pdf?la=en](https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Draft-AG-on-Key-Provisions/Draft-Advisory-Guidelines-on-Key-Provisions-of-the-PDP-(Amendment)-Bill-(20-Nov-2020).pdf?la=en).

¹⁹ *PDPC* (o. FuBn. 18), S. 6.

c) Deemed Consent by Notification

Mit dem „deemed consent by notification“²⁰ führt Sec. 15A N-PDPA²¹ einen weiteren Tatbestand der fingierten Einwilligung ein. Die neue Regelung betrifft Fälle, in denen die Datenverarbeitung auf die Inaktivität einer Person bzw. das Unterlassen eines Widerspruchs gegen die Datenverarbeitung gestützt wird. Sie soll vor allem dann zur Anwendung kommen, 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.²²

Anders als unter dem Regime der DS-GVO, die i.R.d. Einwilligung stets eine eindeutige bestätigende Handlung fordert (Art. 4 Nr. 11 DS-GVO) und damit den Opt-out-Ansatz diesbezüglich untauglich macht,²³ kann ein Unterlassen unter dem PDPA auch bislang im Einzelfall als Einwilligung ausgelegt werden. Da bloße Untätigkeit zumeist aber auf einer ganzen Reihe verschiedener Gründe beruhen kann, ist es sowohl für Organisationen, die Daten verarbeiten möchten, als auch für betroffene Individuen oft schwer vorauszusehen, wann Inaktivität einen entsprechenden Erklärungswert hat.²⁴ Die neue Sec. 15A N-PDPA soll hier Klarheit schaffen. Sie fingiert eine Einwilligung in die Datenverarbeitung bei Untätigkeit unter vier kumulativen Voraussetzungen:

■ Erstens muss eine Organisation vor der beabsichtigten Datenverarbeitung angemessene Schritte unternehmen, um folgende Informationen zur Kenntnis der betroffenen Person zu bringen: die Absicht der Organisation, personenbezogene Daten zu verarbeiten, den Zweck der Datenverarbeitung, eine angemessene Frist, innerhalb derer die Person der Datenverarbeitung widersprechen kann, und eine angemessene Art und Weise, in der ein Widerspruch erklärt werden kann, Sec. 15A Abs. 2 lit. a, Abs. 4 lit. b N-PDPA. Die PDPC hat bereits Kriterien aufgestellt, die herangezogen werden können, um zu beurteilen, ob eine gegenüber einer Person erfolgte Benachrichtigung als angemessen im o.g. Sinne eingestuft werden kann. Für die Angemessenheit spricht etwa, dass eine Organisation die gleiche Kommunikationsmethode nutzt, mit deren Hilfe üblicherweise die Verständigung mit der betroffenen Person stattfindet. Wo Methoden der unmittelbaren Kommunikation mit der betroffenen Person verfügbar sind (z.B. Brief, E-Mail, SMS, Push Notification), sind diese grundsätzlich vorzugswürdig. Insbesondere dann, wenn eine große Anzahl von Personen erreicht werden soll und individuelle Mitteilungen nicht als effektiv eingestuft werden können, kann eine Organisation aber auch auf Wege der Massenkommunikation zurückgreifen. Dazu zählen etwa Veröffentlichungen auf einer Webseite, über Social-Media-Kanäle oder auch in Printmedien.²⁵ Was die Angemessenheit der Länge der Widerspruchsfrist angeht, wird eine Einzelfallbetrachtung durchzuführen sein. Dabei sollten Organisationen wiederum insbesondere das gewählte Medium der Kommunikation in Betracht ziehen, aber auch berücksichtigen, in welchen Abstän-

den eine Interaktion mit der betroffenen Person gewöhnlich erfolgt. Je unmittelbarer das gewählte Medium die Kommunikation herstellt und je einfacher die angebotene Möglichkeit des Widerspruchs ist, desto kürzer wird die Widerspruchsfrist sein dürfen.²⁶

■ Zweitens muss die betroffene Person den Widerspruch gegen die Datenverarbeitung innerhalb der gesetzten Frist unterlassen, Sec. 15A Abs. 2 lit. b N-PDPA.

■ Drittens muss die Organisation vor der Datenverarbeitung eine Bewertung durchgeführt haben, um sicherzustellen, dass die beabsichtigte Datenverarbeitung mit Wahrscheinlichkeit keine nachteiligen Auswirkungen auf die betroffene Person hat, Sec. 15A Abs. 2 lit. a, Abs. 4 lit. a N-PDPA. Dabei muss sie gem. Sec. 15A Abs. 5 lit. a N-PDPA jegliche nachteiligen Effekte, die die Verarbeitung mit Wahrscheinlichkeit auf die betroffene Person haben wird, identifizieren. Als nachteilige Auswirkungen sieht die PDPC dabei nur Effekte an, die eine gewisse Schwelle erreichen. Als Beispiele werden etwa körperliche Schäden, Bedrohungen und Belästigungen sowie schwerwiegende Stresszustände genannt.²⁷ Sind mögliche nachteilige Auswirkungen herausgearbeitet, haben Organisationen angemessene Maßnahmen zu identifizieren und zu implementieren, um diese auszuschließen, die Wahrscheinlichkeit ihres Eintritts zu reduzieren oder um sie abzuschwächen, Sec. 15A Abs. 5 lit. b N-PDPA. Ergibt die Bewertung, dass die Datenverarbeitung trotz dieser Maßnahmen mit einiger Wahrscheinlichkeit negative Effekte auf die betroffene Person haben wird, hat die Datenverarbeitung zu unterbleiben.²⁸ Auf Nachfrage muss eine Organisation der PDPC (nicht aber der betroffenen Person) ihre Bewertung zur Verfügung stellen.²⁹

■ Viertens muss die Organisation weitere noch von der PDPC zu bestimmende Voraussetzungen erfüllen (Sec. 15A Abs. 2 lit. a, Abs. 4 lit. c, Abs. 5 lit. c N-PDPA) und darf weiter mit der Datenverarbeitung keine von der PDPC in den sog. „regulations“ als unzulässig erklärten Zwecke verfolgen, Sec. 15A Abs. 3 N-PDPA. Zu erwarten ist, dass die PDPC in letzterer Hinsicht zumindest ausschließen wird, dass Organisationen über den Opt-out-Ansatz eine fingierte Einwilligung in die Zusendung von Werbenachrichten erlangen.³⁰

2. Vertragserfüllung

Durch Sec. 15 Abs. 3 ff. N-PDPA³¹ wird der PDPA mit dem „deemed consent by contractual necessity“³² um eine weitere Art der fingierten Einwilligung erweitert. Es geht hier um den Bereich der Weitergabe vertragserforderlicher Daten.

Stellt eine Person P einer Organisation A künftig im Hinblick auf einen zwischen den beiden zu schließenden Vertrag personenbezogene Daten zur Verfügung, fingiert der PDPA die Einwilligung von P in die Weitergabe der Daten durch A an dritte Organisationen. Diese dritten Organisationen dürfen die Daten dann wiederum verarbeiten und Gleiches gilt für weitere Organisationen in der Verarbeitungskette. Voraussetzung ist jeweils, dass die Verarbeitung in angemessener Weise für den Vertragsabschluss zwischen P und A notwendig ist, Sec. 15 Abs. 3 und 4 N-PDPA.

Haben P und A bereits einen Vertrag geschlossen, gilt gem. Sec. 15 Abs. 6 N-PDPA Ähnliches für personenbezogene Daten, die A von P mit Blick auf diesen Vertrag zur Verfügung gestellt werden. Die Weitergabe durch A an eine dritte Organisation (sowie die Datenverarbeitung durch diese Organisation) ist dann auf Grund einer fingierten Einwilligung von P erlaubt. Voraussetzung ist, dass sie in angemessener Weise notwendig ist entweder für die Durchführung des Vertrags zwischen P und A oder für den Abschluss oder die Durchführung eines Vertrags zwischen A und der dritten Organisation, der auf Verlangen von P geschlossen wird oder zumindest objektiv im Interesse von P ist.

²⁰ Zum Begriff PDPC (o. Fußn. 18), S. 5.

²¹ Beruhend auf Sec. 7 PDPA-ÄG.

²² PDPC (o. Fußn. 18), S. 9.

²³ Vgl. auch Erwägungsgrund 32 S. 3 DS-GVO.

²⁴ PDPC, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, Stand: 2.6.2020, S. 38, abrufbar unter: [https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-\(2-June-2020\).pdf?la=en](https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-(2-June-2020).pdf?la=en).

²⁵ PDPC (o. Fußn. 18), S. 10 f.

²⁶ PDPC (o. Fußn. 18), S. 11 f.

²⁷ PDPC (o. Fußn. 18), S. 21 f.

²⁸ PDPC (o. Fußn. 18), S. 21.

²⁹ PDPC (o. Fußn. 18), S. 12.

³⁰ PDPC (o. Fußn. 18), S. 14.

³¹ Beruhend auf Sec. 6 PDPA-ÄG.

³² Zum Begriff vgl. PDPC (o. Fußn. 18), S. 5.

Auch hier erfasst die fingierte Einwilligung weitere Organisationen in der Verarbeitungskette, Sec. 15 Abs. 7 N-PDPA.

Die besondere Bedeutung der Regelungen zum „deemed consent by contractual necessity“ liegt wohl vor allem darin, dass sie hinsichtlich der Weitergabe vertragsrelevanter Daten klare Kriterien aufstellen. Zu neuen Ergebnissen wird das allerdings nur teilweise führen. Auch die bisherigen Vorschriften zum „deemed consent by conduct“ konnten in vielen von der neuen Regelung erfassten Fallgestaltungen zu ähnlichen Ergebnissen führen. Das zeigt etwa das Beispiel einer Kreditkartenzahlung im Supermarkt und einer Weitergabe der Zahlungsinformationen durch den Supermarkt an weitere in den Zahlungsvorgang eingebundene Unternehmen (z.B. Banken oder Zahlungsdienstleister). Während die PDPC die Weitergabe der relevanten Daten an diese Unternehmen bislang auf den „deemed consent by conduct“ stützte³³, wird sie künftig wohl auf die neuen Regeln zum „deemed consent by contractual necessity“ zurückgreifen.³⁴ Im Zusammenspiel werden die beiden Fiktionen viele Fälle abdecken können, die i.R.d. DS-GVO vom Erlaubnistatbestand der Vertragserfüllung in Art. 6 Abs. 1 lit. b DS-GVO erfasst sind.

3. Rechtliche Verpflichtungen

Sec. 13 lit. b PDPA bestimmt, dass die Datenverarbeitung erlaubt ist, wenn sie unter dem PDPA oder einem anderen geschriebenen Gesetz erforderlich oder erlaubt ist. Die Regelung ist hinsichtlich rechtlicher Verpflichtungen vergleichbar mit Art. 6 Abs. 1 lit. c DS-GVO.

4. Schutz lebenswichtiger Interessen

Art. 6 Abs. 1 lit. d DS-GVO erklärt eine Verarbeitung als rechtmäßig, die erforderlich ist, um lebenswichtige Interessen einer natürlichen Person zu schützen.

Auch der bisherige PDPA kennt Regelungen, die diesen Bereich betreffen, und führt diese getrennt auf für die Datenerhebung (Sec. 17 Abs. 1 i.V.m. Nr. 1 lit. a und lit. b des Second Schedule zum PDPA), die Datennutzung (Sec. 17 Abs. 2 i.V.m. Nr. 1 lit. a und lit. b des Third Schedule zum PDPA) und die Datenweitergabe (Sec. 17 Abs. 3 i.V.m. Nr. 1 lit. a, lit. b, lit. c und lit. o des Fourth Schedule zum PDPA). Das PDPA-ÄG vereinfacht diese Struktur und regelt die Erlaubnistatbestände für alle Elemente der Datenverarbeitung künftig zusammengefasst in Sec. 17 Abs. 1 N-PDPA³⁵ i.V.m. Part 1 Nr. 1-4 des First Schedule zum N-PDPA³⁶:

- Nr. 1 erlaubt dabei eine Datenverarbeitung, die für einen Zweck erforderlich ist, der klar im Interesse des Betroffenen liegt. Voraussetzung ist, dass die Einwilligung nicht rechtzeitig eingeholt werden kann (Nr. 1 Abs. 1 lit. a) oder die Erteilung der Einwilligung jedenfalls vernünftigerweise zu erwarten ist (Nr. 1 Abs. 1 lit. b). Dabei ist der Betroffene sobald wie möglich über die Datenverarbeitung und deren Zweck zu informieren, Nr. 1 Abs. 2.
- Die Datenverarbeitung, die erforderlich ist, um auf einen lebens-, gesundheits- oder sicherheitsbedrohlichen Notfall zu reagieren, wird durch Nr. 2 ermöglicht.
- Liegt ein solcher Notfall nicht vor, gibt es aber dennoch vernünftige Gründe dafür, anzunehmen, dass die Gesundheit oder Sicherheit einer Person schwerwiegend beeinträchtigt werden wird, und kann eine Einwilligung nicht rechtzeitig eingeholt werden, gestattet Nr. 3 die Datenverarbeitung.
- Die Erlaubnis zur Datenverarbeitung, um einen Freund oder Angehörigen einer verletzten, kranken oder verstorbenen Person zu kontaktieren, ergibt sich aus Nr. 4.

5. Öffentliches Interesse oder hoheitliche Gewalt

Art. 6 Abs. 1 lit. e DS-GVO erklärt eine Verarbeitung als rechtmäßig, die für die Wahrnehmung einer Aufgabe erforderlich ist,

die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die einem Verantwortlichen übertragen wurde. Der Tatbestand erlaubt zunächst die Datenverarbeitung durch Behörden. Aber auch die eigenverantwortliche Datenverarbeitung durch private natürliche oder juristische Personen, denen eine entsprechende Aufgabe übertragen wurde, ist erfasst.³⁷

Im Rahmen der jetzigen Fassung des PDPA stellt sich die Frage nach einer Grundlage für die Datenverarbeitung durch Behörden und private Organisationen, die Daten im Auftrag einer Behörde verarbeiten, nicht. Sec. 4 Abs. 1 lit. c PDPA entzieht die Datenverarbeitung durch diese Verantwortlichen schlichtweg dem Anwendungsbereich der Datenschutzvorschriften.

Sec. 3 lit. b PDPA-ÄG stellt nun allerdings klar, dass diese Privilegierung künftig nur noch für Behörden selbst gilt. Für private Organisationen, die im Auftrag einer Behörde handeln, werden in Zukunft die allgemeinen Vorschriften gelten. Dabei werden sie sich insbesondere auf die folgenden, öffentlichen Interessen dienenden Erlaubnistatbestände berufen können, die jeweils i.V.m. Sec. 17 Abs. 1 N-PDPA zu lesen sind:

- Part 2 Nr. 2 des First Schedule zum N-PDPA erlaubt eine Datenverarbeitung, die im nationalen Interesse liegt. Der Begriff „nationales Interesse“ umfasst dabei die Landesverteidigung, die nationale Sicherheit, die öffentliche Sicherheit, die Aufrechterhaltung wesentlicher Dienste und die Führung internationaler Angelegenheiten, Sec. 2 Abs. 1 PDPA.
- Part 3 Nr. 3 des First Schedule zum N-PDPA erlaubt eine Datenverarbeitung, die zur Durchführung von bestimmten Ermittlungen oder zivil-, straf- oder verwaltungsrechtlichen Verfahren notwendig ist. Diese Ermittlungen/Verfahren können sich etwa auf einen Verstoß gegen ein schriftliches Gesetz oder eine berufliche Verhaltensregel beziehen, Sec. 2 Abs. 1 PDPA.
- Part 1 Nr. 1 und Part 2 Division 1 Nr. 1 des Second Schedule zum N-PDPA erlauben die Erhebung und Nutzung von Daten, die eine Organisation von einer Behörde für einen bestimmten Zweck erhalten hat, für eben diesen Zweck.
- Die Vorschriften des Part 3 Division 1 des Second Schedule zum N-PDPA erlauben in bestimmten Fällen die Weitergabe personenbezogener Daten an Behörden.

6. Wahrung berechtigter Interessen

a) Allgemeiner Tatbestand

Art. 6 Abs. 1 lit. f DS-GVO erlaubt die Datenverarbeitung, die zur Wahrung berechtigter Interessen erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Ein hiermit vergleichbarer Erlaubnistatbestand fehlt im derzeitigen PDPA, sodass Organisationen bislang nur auf die abschließenden Spezialtatbestände zum Schutz berechtigter Interessen zurückgreifen können (s. unter III.6.b)).

Sec. 31 PDPA-ÄG schafft diesbezüglich Abhilfe und führt mit Part 3 Nr. 1 des First Schedule zum N-PDPA eine allgemeine Erlaubnis zur Datenverarbeitung zur Wahrung berechtigter Interessen ein. Absatz 1 der Regelung ermöglicht die Datenverarbeitung, wenn diese einem solchen berechtigten Interesse dient und dieses Interesse jegliche negativen Effekte auf die Person, deren Daten betroffen sind, überwiegt. Letzteres ist vorab i.R.e. Bewertung festzustellen, wobei die Kriterien der Bewertung

³³ PDPC (o. Fußn. 24), S. 42.

³⁴ PDPC (o. Fußn. 18), S. 6-8.

³⁵ Beruhend auf Sec. 8 PDPA-ÄG.

³⁶ Beruhend auf Sec. 31 PDPA-ÄG.

³⁷ Plath, in: Plath, DSGVO/BDSG, 3. Aufl. 2018, Art. 6 DSGVO Rn. 45.

größtenteils identisch sind mit denjenigen, die i.R.d. „deemed consent by notification“³⁸ anzulegen sind, Absatz 2 lit. a i.V.m. Absatz 3. Der grundlegende Unterschied liegt aber darin, dass für einen Rückgriff auf die Regelungen zum „deemed consent by notification“ die Wahrscheinlichkeit negativer Auswirkungen auf die betroffene Person ausgeschlossen sein muss, während es bei einer Datenverarbeitung zur Wahrung berechtigter Interessen lediglich erforderlich ist, dass diese Auswirkungen i.R.e. Abwägung zurücktreten.³⁹ Auch hier muss die Bewertung der PDPC, aber wiederum nicht den betroffenen Personen, auf Nachfrage zur Verfügung gestellt werden.⁴⁰ Gemäß Absatz 2 lit. b müssen Organisationen die betroffenen Personen lediglich in angemessener Weise darüber informieren, dass sie Daten auf Grund der Ausnahmeregelung für berechnete Interessen verarbeiten.

Als berechtigtes Interesse zählt, wie unter der der DS-GVO, jedes von der Rechtsordnung anerkannte Interesse.⁴¹ Das muss gemäß Absatz 1 lit. a nicht zwingend das Interesse der datenverarbeitenden Organisation sein. Auch das Interesse anderer Organisationen, bestimmter Personen oder Personengruppen oder gar der Öffentlichkeit als solcher können herangezogen werden.⁴² Beispiele für berechnete Interessen sind etwa die Aufdeckung und Verhinderung illegaler Aktivitäten (z.B. Betrug oder Geldwäsche) oder von Bedrohungen für Leib, Leben oder Sicherheit sowie die Gewährleistung der IT- und Netzwerksicherheit, die Verhinderung eines Missbrauchs von Diensten und die Durchführung einer Due Diligence Prüfung auf Unternehmensebene.⁴³ Hingegen kann die Ausnahmeregelung – anders als Art. 6 Abs. 1 lit. f DS-GVO⁴⁴ – grundsätzlich nicht herangezogen werden, um Werbenachrichten an Personen zu versenden, Abs. 4 i.V.m. Sec. 37 Abs. 6 N-PDPA⁴⁵ i.V.m. dem Tenth Schedule zum N-PDPA⁴⁶.

b) Spezialtatbestände

Neben dem neuen allgemeinen Tatbestand listet der N-PDPA auch weiterhin Spezialtatbestände zur Wahrung berechtigter Interessen auf. Sie werden vor allem aufgeführt in Part 3 Nr. 2-10 des First Schedule zum N-PDPA. Privilegiert werden so insbesondere Datenverarbeitungsvorgänge, die notwendig sind für Evaluierungszwecke (Nr. 2), die Eintreibung oder Begleichung von Schulden (Nr. 4) und die Erbringung und den Bezug von Rechtsdienstleistungen (Nr. 5). Außerdem werden Verarbeitungsvorgänge erlaubt, die im Hinblick auf den Eintritt in ein Arbeitsverhältnis sowie dessen Administration und Beendigung angemessen sind (Nr. 10). Darüber hinaus gestatten Part 2 Division 3 und Part 3 Division 2 des Second Schedule zum N-PDPA die Datennutzung und Weitergabe zu Forschungszwecken. Part 4 des First Schedule zum N-PDPA enthält außerdem ausführliche Regelungen zur Datenverarbeitung für den M&A-Bereich.

Ausführlicher vorgestellt werden soll hier die in Part 2 Division 2 Nr. 1 des Second Schedule zum N-PDPA neu eingeführte Erlaubnis der Datennutzung zu Zwecken der Geschäftsoptimierung. Als Geschäftsoptimierung gelten nach deren Absatz 1 vier Bereiche:

- die Entwicklung oder Verbesserung von Waren und Dienstleistungen der Organisation,
- die Entwicklung oder Verbesserung von operativen Methoden und Prozessen der Organisation,
- die Analyse des Verhaltens und der Vorlieben von Personen hinsichtlich der Waren und Dienstleistungen der Organisation und
- die Identifizierung von Waren oder Dienstleistungen der Organisation, die für bestimmte Personen geeignet sind, sowie die Personalisierung dieser Waren oder Dienstleistungen.

Zu diesen vier Geschäftsoptimierungszwecken dürfen Organisationen künftig personenbezogene Daten, die sie im Einklang mit den allgemeinen Vorschriften für einen beliebigen Zweck erhoben haben, nutzen, wenn der jeweilige Geschäftsoptimierungszweck vernünftigerweise nicht ohne die Verarbeitung der Daten in einer individuell identifizierbaren Form erreicht werden kann und die Datennutzung angemessen ist, Nr. 1 Abs. 3.

Die Privilegierung gilt ausweislich Nr. 1 Abs. 4 nicht für „corporations“ i.S.d. Sec. 4 Abs. 1 des singapurischen Companies Act⁴⁷ und damit etwa nicht für die singapurische „private company limited by shares“, die in Grundzügen mit der deutschen GmbH vergleichbar ist. Die PDPC scheint „corporations“ aber, über den Wortlaut hinaus, die Datennutzung zu Geschäftsoptimierungszwecken auf Grundlage von Part 5 Nr. 1 des First Schedule zum N-PDPA zu erlauben.⁴⁸

Nach seinem Wortlaut privilegiert Part 5 Nr. 1 des First Schedule zum N-PDPA allerdings lediglich die zu Geschäftsoptimierungszwecken erfolgende Weitergabe personenbezogener Daten einer „corporation“ Y an eine verbundenes Unternehmen, „corporation“ X, sowie die Erhebung und Nutzung dieser Daten durch X. Diese Datenverarbeitungsvorgänge dürfen dabei nur erfolgen, wenn die oben für die Datennutzung beschriebenen Einschränkungen beachtet werden, Nr. 1 Abs. 3 lit. a und lit. b, Nr. 1 Abs. 4. Zusätzlich müssen verbindliche Vereinbarungen oder Regeln zwischen X und Y bestehen, die die Implementierung und Aufrechterhaltung angemessener Schutzmaßnahmen hinsichtlich der personenbezogenen Daten durch X sicherstellen, Nr. 1 Abs. 3 lit. c. Die Datenweitergabe/-erhebung zu den oben vorgestellten dritten und vierten Geschäftsoptimierungsbereichen ist zusätzlich nur privilegiert, wenn es sich bei der betroffenen Person um einen Kunden von Y oder einen zumindest möglichen Kunden von X handelt, Nr. 1 Abs. 5.

Keinesfalls kann die Privilegierung von Geschäftsoptimierungszwecken herangezogen werden, um Werbenachrichten an Personen zu versenden, Part 5 Nr. 1 Abs. 6 des First Schedule zum N-PDPA und Part 2 Division 2 Nr. 1 Abs. 3 des Second Schedule zum N-PDPA.

7. Exkurs: Übermittlung personenbezogener Daten an Empfänger in einem Drittland

Auf Grund der besonderen Relevanz für internationale Unternehmensgruppen soll an dieser Stelle ergänzend hervorgehoben werden, dass der PDPA – genau wie die DS-GVO – für eine Übermittlung personenbezogener Daten an Empfänger in Drittländern Voraussetzungen kennt, die über die bloße Erfüllung eines Erlaubnistatbestands hinausgehen. Organisationen dürfen personenbezogene Daten nur dann ins Ausland übermitteln, wenn sichergestellt ist, dass die Daten im Drittland einen Schutzstandard genießen, der mit dem des PDPA vergleichbar ist, Sec. 26 Abs. 1 PDPA. Die datenübermittelnde Organisation hat also dafür Sorge zu tragen, dass der Datenempfänger im Drittland rechtlich gebunden ist, einen solchen vergleichbaren Schutzstandard zu gewähren, Reg. 9 Abs. 1 lit. b Personal Data Protection Regulations 2014 (PDPR)⁴⁹. Im Hinblick auf den allgemein relativ geringen Schutzstandard des PDPA wird diese Vo-

³⁸ S. unter III.1.c).

³⁹ PDPC (o. FuBn. 18), S. 21.

⁴⁰ PDPC (o. FuBn. 18), S. 17.

⁴¹ PDPC (o. FuBn. 18), S. 15; zur DS-GVO Plath (o. FuBn. 37), Art. 6 DSGVO Rn. 54.

⁴² PDPC (o. FuBn. 18), S. 16.

⁴³ PDPC (o. FuBn. 18), S. 18.

⁴⁴ Erwägungsgrund 47 S. 7 DS-GVO.

⁴⁵ Beruhend auf Sec. 17 PDPA-ÄG.

⁴⁶ Beruhend auf Sec. 38 PDPA-ÄG.

⁴⁷ Abrufbar unter: <https://sso.agc.gov.sg/Act/CoA1967#pr4->

⁴⁸ PDPC (o. FuBn. 18), S. 23.

⁴⁹ Abrufbar unter: <https://sso.agc.gov.sg/SL/PDPA2012-S362-2014?DocDate=20140519#pr9->

raussetzung bei einem Empfänger im Anwendungsbereich der DS-GVO, so etwa bei einem Unternehmen in Deutschland, ohne Weiteres erfüllt sein.⁵⁰ Wo die im Land des Empfängers geltenden Gesetze hingegen keinen vergleichbaren Schutz gewähren, bietet es sich z.B. an, den Datenempfänger vertraglich zur Gewährung des notwendigen Schutzstandards zu verpflichten, Reg. 10 Abs. 1 lit. b, Abs. 2 PDPR. Darüber hinaus wird gem. Reg. 9 Abs. 3 PDPR aber auch ohne die Gewährung eines vergleichbaren Schutzes in einigen Fällen fingiert, dass die singapurische Organisation ihre Verpflichtungen aus Reg. 9 Abs. 1 lit. b PDPR erfüllt hat. Das gilt vor allem dann, wenn der betroffenen Person ein angemessener schriftlicher Überblick über das Schutzniveau im Land des Empfängers zur Verfügung gestellt wurde und sie der Datenübermittlung an eben diesen Empfänger nachfolgend (dennoch) zugestimmt hat, Reg. 9 Abs. 3 lit. a, Abs. 4 lit. a PDPR.

IV. Fazit

Das PDPA-ÄG reformiert die Tatbestände, auf die in Singapur aktive Organisationen die Erhebung, Nutzung und Weitergabe personenbezogener Daten stützen können. Vor allem die Einführung einer fingierten Einwilligung im Bereich der Vertragserfüllung sowie eines allgemeinen Erlaubnistatbestands zur Wahrung berechtigter Interessen führt dabei zu einer stark praxisrelevanten Angleichung der Erlaubnistatbestände von PDPA und DS-GVO. Bei allen alten und neuen Parallelen darf aber dennoch

nicht übersehen werden, dass die beiden Gesetze zwar vergleichbar, aber eben nicht gleich sind. Datenverarbeitungen, die unter dem Regime der DS-GVO erlaubt, unter dem PDPA aber ohne Erfüllung weiterer Voraussetzungen verboten sind, wird es weiterhin geben. Gleiches gilt umgekehrt.

Schnell gelesen ...

- Die Erlaubnistatbestände im singapurischen Datenschutzrecht werden erweitert und umgestaltet.
- Teilweise findet dadurch eine Angleichung an die Erlaubnistatbestände der DS-GVO statt.
- In Singapur aktive deutsche Unternehmen sollten sich mit den Gesetzesänderungen auseinandersetzen, um herauszufinden, wo Datenverarbeitungsvorgänge nun eventuell gruppenweit auf eine ähnliche Basis gestützt werden können und wo dies weiterhin nicht möglich ist.



Sebastian Blasius arbeitet als Rechtsanwalt in Singapur.

⁵⁰ Vgl. auch *Lim* (o. Fußn. 10), S. 338.