SEBASTIAN BLASIUS

Grundlagen der Compliance mit dem singapurischen Datenschutzrecht

Elementare Anforderungen und Vergleich mit der DS-GVO

Rechtsvergleich
Datenschutzbeauftragter
Verzeichnis von Verarbeitungstätigkeiten
Datenschutz-Folgenabschätzung
Auftragsverarbeitung

■ Die materiellen Vorschriften des singapurischen Datenschutzgesetzes sind im Vergleich zur DS-GVO ausgesprochen kurzgehalten. Sie werden allerdings durch Leitfäden ergänzt, die die lokale Datenschutzkommission erlässt und in denen sie ihre Interpretation der gesetzlichen Vorgaben darlegt. In grundlegenden Bereichen führt das zu Konzepten, die mit denen der DS-GVO vergleichbar sind. Dieser Beitrag analysiert die Anforderungen hinsichtlich der Benennung eines Datenschutzbeauftragten, der Führung eines Verzeichnisses von Verarbeitungstätigkeiten, der Durchführung von Datenschutz-Folgenabschätzungen und der Auftragsverarbeitung. Er vermittelt deutschen Unternehmen, die in Singapur aktiv sind, so ein wichtiges Verständnis zu grundlegenden Compliance-Bausteinen.

■ The substantive provisions of Singapore's data protection law are extremely short compared to the GDPR. However, they are supplemented by advisory guidelines in which the local Personal Data Protection Commission sets out its interpretation of the legal requirements. In fundamental areas, this leads to concepts that are comparable to those of the GDPR. This article analyses the requirements to appoint a data protection officer, to maintain a record of processing activities, to conduct data protection impact assessments and to properly manage data processors. It thus provides German companies operating in Singapore with an important understanding of the basic building blocks of compliance.
Lesedauer: 21 Minuten

I. Einführung

Der Personal Data Protection Act 2012 (PDPA)[1] ist das singapurische Äquivalent zur DS-GVO. Die Hauptpflichten, die Organisationen beim Umgang mit personenbezogenen Daten treffen, fasst das Gesetz in nur 23 Vorschriften zusammen.[2] Damit ist der PDPA bedeutend weniger detailliert ausgestaltet als die europäische Verordnung. Das macht eine umfangreiche Auslegung des Gesetzestexts notwendig und die Personal Data Protection Commission (PDPC), die gem. Sec. 5 Abs. 2 PDPA für die Administration des PDPA zuständig ist, legt ihre Interpretation in einer stets wachsenden Anzahl von Leitfäden zu verschiedenen Themen dar.[3] Diese spiegeln oft Konzepte wider, die sich in der DS-GVO in vergleichbarer Weise direkt aus dem Gesetz ergeben.

Für Rechtsadressaten ist die Kombination aus knappen gesetzlichen Vorgaben und mittlerweile 29 Leitfäden nicht leicht zu überblicken. Viele Verpflichtungen, die ihren ausdrücklichen Niederschlag nicht im PDPA, sondern ausschließlich in Leitfäden gefunden haben, sind singapurischen Organisationen schlichtweg unbekannt. Das führt fast zwangsläufig zu Gesetzesbrüchen. Besonders betroffen sind hierbei u.a. lokale Tochtergesellschaften von ausländischen (inklusive deutschen) kleinen und mittleren Unternehmen (KMU). In diesen Einheiten konzentriert sich die Belegschaft zumeist gänzlich auf das operative Geschäft. Die Einhaltung der Regeln des PDPA spielt dann bestenfalls eine untergeordnete Rolle und es kommt schon im datenschutzrechtlichen Unterbau zu gravierenden Mängeln. Dabei lassen sich Grundbausteine der singapurischen Datenschutz-Compliance recht einfach zusammenfassen: Organisationen sollten eine Person damit betrauen, die Einhaltung des PDPA sicherzustellen, wissen und dokumentieren, welche personenbezogenen Daten sie wie verarbeiten, die sich daraus ergebenden rechtlichen Risiken bewerten und angemessen adressieren sowie Dritte, die sie mit der Verarbeitung personenbezogener Daten beauftragen, adäquat auswählen, führen und kontrollieren.

Der vorliegende Beitrag analysiert diese grundlegenden Anforderungen im Detail und zieht, wo es sich anbietet, Parallelen zur DS-GVO. Die beschriebenen Konzepte können Unternehmen in Singapur damit als solide Basis für ihre Compliance dienen.

II. Die Compliance-Grundlagen des singapurischen Datenschutzrechts

1. Datenschutzbeauftragter

Datenschutzbeauftragten obliegt generell die Aufgabe, die Einhaltung datenschutzrechtlicher Vorschriften in einem Unternehmen sicherzustellen.[4]

Geht es um das „Ob" der Benennung eines Datenschutzbeauftragten, sind die Vorschriften des PDPA strenger als die der DS-GVO. Gem. Art. 37 Abs. 1 lit. b und lit. c DS-GVO hängt die Bestellpflicht im privaten Sektor von der Kerntätigkeit eines Unternehmens ab. Nur wenn diese aus Verarbeitungsvorgängen besteht, die „aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen" oder die sich auf die umfangreiche „Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 [DS-GVO] oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 [DS-GVO]" erstrecken, muss ein Datenschutzbeauftragter benannt werden. Im Gegensatz dazu sieht Sec. 11 Abs. 3 PDPA für sämtliche Organisationen im Anwendungsbereich des PDPA die Pflicht vor, einen oder mehrere Datenschutzbeauftragte zu benennen. Ausnahmen für Unternehmen, deren Datenverarbeitungsvorgänge unterhalb einer gewissen Relevanzschwelle liegen, gibt es nicht. Insbesondere bei den in Singapur vielfach anzutreffenden Holding-Gesellschaften ohne Beschäftigte stößt dies bisweilen auf Erstaunen. In der Praxis herrscht hier häufig die Ansicht vor, man verarbeite keine personenbezogenen Daten und benötige daher auch keinen Datenschutzbeauftragten. Übersehen werden dabei die Daten, die Unternehmen bereits auf Grund ihrer gesellschaftsrechtlichen Struktur oder gesetzlicher Vorschriften erheben

1 Abrufbar unter: https://sso.agc.gov.sg/Act/PDPA2012#legis.
2 S. Sec. 11–26E PDPA.
3 Sämtliche Leitfäden sind abrufbar unter: https://www.pdpc.gov.sg/Guidelines-and-Consultation?type=advisory-guidelines.
4 S. insb. Sec. 11 Abs. 3 PDPA und Art. 39 Abs. 1 lit. b DS-GVO.

müssen. Dazu zählen etwa die personenbezogenen Daten von Gesellschaftern (wenn diese natürliche Personen sind), von Geschäftsführern und von wirtschaftlich Berechtigten (Ultimate Beneficial Owners)[5].

Die geschäftlichen Kontaktinformationen (Business Contact Information)[6] zumindest eines Datenschutzbeauftragten müssen der Öffentlichkeit zugänglich gemacht werden, Sec. 11 Abs. 5 PDPA. Ausreichend ist hierfür etwa ihre Publikation auf der offiziellen Unternehmenswebseite, Sec. 11 Abs. 5A PDPA iVm Sec. 1A Abs. 1 lit. b Personal Data Protection Regulations 2021[7] (PDPR). Ihre Mitteilung an eine Aufsichtsbehörde ist, anders als nach Art. 37 Abs. 7 DS-GVO, nicht verpflichtend. Sie wird aber von der PDPC empfohlen[8] und ist in der Praxis auch gängig. Sec. 11 Abs. 5A PDPA iVm Sec. 1A Abs. 1 lit. a PDPR stellen klar, dass auch die Hinterlegung der Kontaktdaten in einem von der Accounting and Corporate Regulatory Authority geführten und mit dem deutschen Handelsregister vergleichbaren Verzeichnis die Voraussetzungen an die Veröffentlichung erfüllt. Während es nicht zwingend ist, dass der Datenschutzbeauftragte, dessen Kontaktinformationen veröffentlicht werden, in Singapur ansässig ist, muss er aus Sicht der Kommission zu singapurischen Geschäftszeiten über die veröffentlichten Kontaktinformationen erreichbar sein.[9] Außerdem müssen angegebene Telefonnummern aus dem singapurischen Nummernraum stammen.[10] Diese Voraussetzungen werden etwa bei einem in Deutschland ansässigen Datenschutzbeauftragten nur schwierig zu erfüllen sein.

Bei der Auswahl der Person, die die Funktion des Datenschutzbeauftragten übernehmen soll, lassen sich Unternehmen immer wieder von einem verkürzten Verständnis datenschutzrechtlicher Anforderungen leiten. So fällt die „natürliche Wahl" nicht selten auf einen Mitarbeiter aus dem IT-Team. Dieser mag zwar seinen technischen Fachbereich beherrschen, hat aber in der Praxis üblicherweise nur wenige oder gar keine Kenntnisse hinsichtlich rechtlicher Datenschutzfragen. Das ist problematisch. Zwar gibt es im PDPA keine Regel, die ähnliche Anforderungen wie Art. 37 Abs. 5 DS-GVO stellt und ausführt, dass der Datenschutzbeauftragte auf Grund seiner beruflichen Qualifikation, seines Fachwissens und seiner Fähigkeit zur Erfüllung der gesetzlich vorgesehenen Aufgaben benannt werden muss. Allerdings besteht auch nach dem PDPA die Pflicht zur Bestellung eines Datenschutzbeauftragten mit der klaren Zielsetzung, dass dieser für die Datenschutz-Compliance des ihn bestellenden Unternehmens verantwortlich sein soll. Daraus ergibt sich notwendigerweise, dass er die hierzu erforderlichen Kenntnisse und Fähigkeiten haben muss.[11] In ihren Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Key Concepts Guidelines) konkretisiert die Kommission das weiter dahingehend, dass Datenschutzbeauftragte geschult und zertifiziert sein müssen.[12] Als Beispiel für ein akzeptables Zertifikat nennen die Key Concepts Guidelines das Practitioner Certificate for Personal Data Protection (Singapore), das die PDPC gemeinsam mit der International Association of Privacy Professionals (IAPP) verleiht.[13] Darüber hinaus finden sich auf der Webseite der PDPC weitere Informationen zu den möglicherweise notwendigen Kompetenzen eines Datenschutzbeauftragten sowie zu möglichen Schulungen und Zertifizierungen.[14] In jedem Fall sollten Unternehmen darauf achten, dass der Datenschutzbeauftragte die notwendigen Kenntnisse spezifisch im singapurischen Datenschutzrecht aufweist. Daran fehlt es zuhauf bei Organisationen mit deutschen Wurzeln, die die Funktion nicht lokal besetzen, sondern sie vom – idR „nur" mit der DS-GVO vertrauten – Datenschutzbeauftragten der Muttergesellschaft ausüben lassen.

Unternehmen, die einen Datenschutzbeauftragten benennen, ohne zu beachten, dass dieser bestimmte Kenntnisse und Fähigkeiten haben muss, sind vielfach auch mit der Stellung, die dieser innerhalb ihrer Organisation haben sollte, und mit den Aufgaben, die die Position mit sich bringt, nicht vertraut. Auch das mag dadurch begünstigt sein, dass der PDPA – anders als die DS-GVO in ihren Art. 38 und 39 DS-GVO – hierzu schweigt. Ein Rückgriff auf die Key Concepts Guidelines schafft jedoch erneut Klarheit. Danach müssen Datenschutzbeauftragte über ausreichende Befugnisse verfügen, um ihre Aufgaben wahrnehmen zu können, und entweder selbst Mitglied der Geschäftsführung sein oder direkt an diese berichten.[15] Neben der allgemeinen Stellung als interner Experte für Datenschutzfragen fallen idR folgende Tätigkeiten in den Verantwortungsbereich des Datenschutzbeauftragten:

- Zusammenarbeit mit der Geschäftsleitung und einzelnen Unternehmensabteilungen bei der Entwicklung und Implementierung geeigneter Datenschutzrichtlinien,
- Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten[16] oder Unterstützung hierbei,
- Durchführung von Datenschutz-Folgenabschätzungen[17],
- Überwachung und Meldung von Datenschutzrisiken,
- Durchführung interner Schulungen zur Datenschutz-Compliance,
- Abstimmung zu Datenschutzfragen mit Vertretern verschiedener Interessensgruppen und
- Zusammenarbeit mit dem für IT-Sicherheit zuständigen Team (oder Übernahme dieser Funktion).[18]

Wenn Unternehmen einen ihrer Mitarbeiter zusätzlich zu seinem normalen Aufgabenbereich zum Datenschutzbeauftragten bestellen, werden die o.g. Aufgabenbereiche in vielen Fällen nur stark unzureichend abgedeckt. Hier sind Organisationen gut beraten, die Funktion an externe Experten auszugliedern oder diese zumindest zur Beratung hinzuzuziehen.

2. Verzeichnis von Verarbeitungstätigkeiten

Ein Verzeichnis der Verarbeitungstätigkeiten eines Unternehmens – im singapurischen Datenschutzrecht teilweise als Perso-

5 Ausführliche Informationen zum Register of Registrable Controllers, in dem die wirtschaftlich Berechtigten geführt werden müssen, finden sich etwa auf der Webseite der singapurischen Accounting and Corporate Regulatory Authority, s. https://www.acra.gov.sg/legislation/legislative-reform/companies-act-reform/companies-amendment-act-2017/register-of-registrable-controllers.

6 Zum Begriff s. Sec. 2 Abs. 1 PDPA.

7 Abrufbar unter: https://sso.agc.gov.sg/SL/PDPA2012-S63-2021?DocDate=20210930.

8 PDPC, Webseite, abrufbar unter: https://www.pdpc.gov.sg/FAQ-Listing?persona=dp-professional&topic=data-protection-officers&page=1.

9 S.a. PDPC, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, Stand: 16.5.2022, Abschnitt 21.7, 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-17-May-2022.ashx?la=en. An anderer Stelle geht die PDPC gar so weit, zu fordern, dass der Datenschutzbeauftragte, dessen Kontaktinformationen veröffentlicht werden, erreichbar sein muss, wann auch immer ein Mitglied der singapurischen Öffentlichkeit versucht, ihn zu erreichen; s. PDPC, Webseite, abrufbar unter: https://www.pdpc.gov.sg/FAQ-Listing?persona=dp-professional/ftopic=data-protection-officer&page=1.

10 PDPC, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, Stand: 16.5.2022, Abschnitt 21.7.

11 S.a. PDPC, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, Stand: 16.5.2022, Abschnitt 21.5.

12 PDPC, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, Stand: 16.5.2022, Abschnitt 21.5.

13 PDPC, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, Stand: 16.5.2022, Abschnitt 21.5, dort Fußn. 84.

14 PDPC, Webseite, abrufbar unter: https://www.pdpc.gov.sg/Help-and-Resources/2020/03/DPO-Competency-Framework-and-Training-Roadmap.

15 PDPC, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, Stand: 16.5.2022, Abschnitt 21.5.

16 S. unter II.2.

17 S. unter II.3.

18 PDPC, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, Stand: 16.5.2022, Abschnitt 21.4.

nal Data Inventory bezeichnet[19] – bildet eine unverzichtbare Grundlage für die Datenschutz-Compliance eines Unternehmens. Dennoch wird ein solches Verzeichnis in der Praxis oftmals nicht erstellt, sodass viele Unternehmen allenfalls eine vage Vorstellung hinsichtlich ihrer Verarbeitungstätigkeiten haben. Die fast zwangsläufige Folge sind Compliance-Lücken. Der Grund für die unterlassene Führung des Verzeichnisses mag wiederum in den kurzen Vorschriften des PDPA liegen. Während die DS-GVO die Führung eines Verzeichnisses von Verarbeitungstätigkeiten zumindest für Unternehmen ab 250 Mitarbeitern zwingend vorschreibt (Art. 30 DS-GVO), adressiert das singapurische Datenschutzgesetz das Thema nicht ausdrücklich. Und selbst der von der PDPC veröffentlichte Guide to Developing a Data Protection Management Programme (DPMP Guide) spricht lediglich eine Empfehlung zur Führung eines Personal Data Inventory aus.[20] In ihren Entscheidungen über mögliche PDPA-Verletzungsfälle, die die PDPC in Ausübung ihrer quasi-gerichtlichen Befugnisse trifft, wird die Kommission hingegen zunehmend deutlicher und beschreibt die Führung eines Personal Data Inventory als Grundvoraussetzung für die Erfüllung der im PDPA vorgesehenen Protection Obligation.[21] Diese besagt, dass Organisationen angemessene Sicherheitsvorkehrungen treffen müssen, um personenbezogene Daten in ihrem Besitz oder unter ihrer Kontrolle zu schützen, Sec. 24 PDPA. Während die PDPC die o.g. Position ausdrücklich mit Blick auf Organisationen einnahm, die über umfangreiche personenbezogenen Daten verfügen, lässt sich der zu Grunde liegende Gedankengang unabhängig vom Datenvolumen verallgemeinern: Nur wer weiß, welche personenbezogenen Daten er wie und für welche Zwecke erhebt, nutzt und weitergibt, kann diese auch im Einklang mit den gesetzlichen Vorschriften verarbeiten und schützen.[22] Und auch die sachgemäße Gewährung von Betroffenenrechten wird ohne ein Personal Data Inventory nur schwerlich möglich sein. Das gilt insbesondere für die Rechte auf Auskunft (Sec. 21 PDPA) und Berichtigung (Sec. 22 PDPA).

Aus dem DPMP Guide[23] sowie einem von der PDPC zur Verfügung gestellten Musterverzeichnis[24] ergibt sich ein Vorschlag hinsichtlich der Angaben, die in ein Personal Data Inventory aufgenommen werden sollten:

- Unternehmensabteilungen/-funktionen, die für die Datenverarbeitung zuständig sind,
- Kategorien betroffener Personen,
- Kategorien personenbezogener Daten,
- Vorliegen einer Einwilligung der betroffenen Personen,
- Zwecke der Datenerhebung,
- Entscheidungsträger und Verantwortlicher hinsichtlich der Datenverarbeitung (Data Owner),
- Unternehmensabteilungen/-funktionen, die die Daten erheben,
- Medium der Datenerhebung,
- Unternehmensabteilungen/-funktionen, die die Daten nutzen,
- Unternehmensabteilungen/-funktionen, die Zugriff auf die Daten haben,
- externe Parteien innerhalb und außerhalb Singapurs, gegenüber denen die personenbezogenen Daten offengelegt werden, sowie die Mittel der Offenlegung,
- Formen physischer und digitaler Datenspeicherung,
- Fristen für die Datenanonymisierung-/löschung und
- Löschungsmethoden.

Die genannten Kategorien können (und sollten) an die Bedürfnisse und Verarbeitungstätigkeiten der jeweiligen Organisation angepasst werden. Unternehmen, deren Datenverarbeitungsvorgänge nicht nur dem PDPA, sondern zusätzlich auch der DS-GVO unterliegen, sollten hierbei darauf achten, dass zumindest die in Art. 30 DS-GVO vorgesehenen Angaben abgedeckt werden. Außerdem erscheint etwa die Frage nach dem Vorliegen einer Einwilligung der betroffenen Person angesichts der Vielzahl möglicher PDPA-Erlaubnistatbestände für eine Datenverarbeitung[25] als zu eng. Das gilt insbesondere, nachdem Unternehmen ihre Datenverarbeitungstätigkeiten seit dem Jahr 2021 auch auf die Verfolgung berechtigter Interessen stützen können (s. Sec. 17 Abs. 1 PDPA iVm Part 3 Nr. 1 des First Schedule zum PDPA). Ähnlich wie unter dem Regime der DS-GVO, die eine entsprechende Rechtsgrundlage in ihrem Art. 6 Abs. 1 lit. f DS-GVO enthält, ist zu erwarten, dass die Bedeutung der Einwilligung als Verarbeitungsgrundlage stark verblassen wird.

3. Datenschutz-Folgenabschätzungen

Auch eine Verpflichtung zur Durchführung und Dokumentierung einer Datenschutz-Folgenabschätzung (DSFA) sieht der PDPA anders als die DS-GVO (s. Art. 35 DS-GVO) nicht ausdrücklich vor. Sie wird daher in der Praxis insbesondere in KMU vielfach gänzlich unterlassen bzw. bestenfalls unvollständig durchgeführt. Genau wie die Führung eines Personal Data Inventory ist aber auch die Durchführung von DSFA als Grundvoraussetzung für eine gesetzeskonforme Datenverarbeitung anzusehen. Dabei gehen das Verzeichnis der Verarbeitungstätigkeiten und die DSFA Hand in Hand: Das Personal Data Inventory beschreibt den datenschutzrechtlich relevanten Sachverhalt; die Datenschutz-Folgenabschätzung bewertet diesen aus rechtlicher Sicht.

Der von der singapurischen Datenschutzkommission erlassene Guide to Data Protection Impact Assessments[26] beschreibt sechs Phasen, die eine DSFA typischerweise durchlaufen sollte und die im Folgenden kurz zusammengefasst werden.

a) Erste Phase

In der ersten Phase wird die Notwendigkeit einer DSFA festgestellt. Diese besteht im Allgemeinen dann, wenn datenschutzrechtlich relevante Prozesse oder Systeme eingeführt, entwickelt, implementiert oder überarbeitet werden oder wenn zusätzliche Kategorien personenbezogener Daten verarbeitet werden sollen. Beispielhaft lässt sich die geplante Inbetriebnahme einer Webseite nennen, über die personenbezogene Daten von Besuchern ebendieser Webseite erhoben werden.[27]

b) Zweite Phase

Die zweite Phase ist der Planung der DSFA gewidmet. Hier sollten die folgenden Punkte beschrieben werden:

- das datenschutzrechtlich relevante Projekt,
- der Umfang und der Hintergrund der DSFA,

19 S. etwa PDPC, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, Stand: 16.5.2022, Abschnitt 21.4.
20 PDPC, Guide to Developing a Data Protection Management Programme, Stand: 14.9.2021, S. 13 und S. 23, abrufbar unter: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPMP/Guide-to-Developing-a-Data-Management-Programme-14-Sep-2021.pdf.
21 PDPC, [2022] SGPDPC 9, S. 7, abrufbar unter: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/GD_Eatigo-International-Pte-Ltd_211222.pdf.
22 Ähnl. PDPC, [2022] SGPDPC 9, S. 2.
23 PDPC, Guide to Developing a Data Protection Management Programme, Stand: 14.9.2021, S. 23.
24 Abrufbar unter: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPMP/Sample-Personal-Data-Inventory-Map-Template.xlsx.
25 Dazu ausf. Blasius ZD 2021, 145.
26 PDPC, Guide to Data Protection Impact Assessments, Stand: 14.9.2021, abrufbar unter: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPIA/Guide-to-Data-Protection-Impact-Assessments-14-Sep-2021.pdf.
27 PDPC, Guide to Data Protection Impact Assessments, Stand: 14.9.2021, S. 12 f.

- die Methodik der Risikobewertung,[28]
- die Involvierung verschiedener Parteien (zB Unternehmensabteilungen oder externe Interessengruppen) und
- der zeitliche Rahmen der DSFA.[29]

c) Dritte Phase

Die dritte Phase dient der umfassenden Identifizierung der involvierten personenbezogenen Daten und Datenströme. Dies erfordert vor allem die Prüfung aller projektbezogenen Dokumente, wie etwa der bestehenden oder zu schließenden Verträge mit dritten Parteien. Außerdem sollten alle relevanten Teams und Abteilungen in den Prozess einbezogen werden. Während die Kommission hervorhebt, dass die Punkte, die in dieser dritten Phase eruiert und dokumentiert werden sollten, mit Blick auf das konkrete Projekt und die organisatorischen Bedürfnisse zu bestimmen sind,[30] bilden die typischen Angaben eines Personal Data Inventory eine solide Basis.[31] Aus praktischer Sicht ist es daher empfehlenswert, die Erstellung eines Personal Data Inventory grundsätzlich mit der Durchführung einer DSFA zu verbinden.

d) Vierte Phase

Die vierte Phase bildet das Herzstück der DSFA. Hier wird zunächst geprüft, ob die projektbezogene Datenverarbeitung den Anforderungen des PDPA und denen etablierter Best Practices genügt. Als Ausgangspunkt kann die Erstellung und Beantwortung eines DSFA-Fragebogens dienen.[32] Der Fragebogen sollte dabei die zehn Hauptpflichten abdecken, die der PDPA Organisationen auferlegt, und grob die folgenden Fragen adressieren:[33]

- Zur Consent Obligation: Kann die relevante Datenerhebung, -nutzung und/oder -weitergabe auf einen Erlaubnistatbestand gestützt werden?[34]
- Zur Notification Obligation: Wurden die betroffenen Personen, wo notwendig, über die Zwecke der Datenverarbeitung informiert?[35]
- Zur Purpose Limitation Obligation: Sind die Zwecke der Datenverarbeitung angemessen und findet die Datenverarbeitung ausschließlich zu Zwecken, über die (wo nötig) informiert wurde, statt?[36]
- Zur Accuracy Obligation: Hat die Organisation, wo nötig, angemessene Maßnahmen implementiert, um sicherzustellen, dass die erhobenen personenbezogenen Daten korrekt und vollständig sind?[37]
- Zur Access and Correction Obligation: Hat die Organisation einen Prozess implementiert, um Gesuche um Auskunft oder Berichtigung personenbezogener Daten zu empfangen und zu adressieren?[38]
- Zur Protection Obligation: Hat die Organisation angemessene Maßnahmen zum Schutz der personenbezogenen Daten in ihrem Besitz oder unter ihrer Kontrolle getroffen?[39]
- Zur Retention Limitation Obligation: Stellt die Organisation sicher, dass sie personenbezogene Daten nur so lange in nichtanonymisierter Form aufbewahrt, wie dies durch den ursprünglichen Zweck der Datenerhebung oder zu rechtlichen oder geschäftlichen Zwecken gerechtfertigt ist?[40]
- Zur Transfer Limitation Obligation: Stellt die Organisation sicher, dass personenbezogene Daten, die in ein Drittland übertragen werden, weiter einen Schutzstandard genießen, der mit dem des PDPA vergleichbar ist?[41]
- Zur Data Breach Notification Obligation: Hat die Organisation eine Richtlinie zur Umsetzung der Meldepflicht bei Verletzungen des Schutzes personenbezogener Daten entworfen und implementiert?[42]
- Zur Accountability Obligation: Hat die Organisation projektbezogene Richtlinien zum Umgang mit personenbezogenen Daten entworfen, implementiert und gegenüber ihrer Belegschaft kommuniziert?[43]

Sind mögliche Compliance-Lücken und -Risiken festgestellt, werden diese hinsichtlich der Schwere ihrer möglichen Folgen und der Wahrscheinlichkeit des Eintritts dieser Folgen anhand der in der zweiten Phase festgelegten Risikobewertungsmethodik kategorisiert.[44] Das dient insbesondere dem Ziel, Risiken zu identifizieren, die sich außerhalb des Toleranzbereichs der Organisation befinden.[45]

e) Fünfte Phase

In der fünften Phase werden in einem Action Plan Maßnahmen entwickelt und dokumentiert, um die zuvor erkannten Risiken angemessen zu adressieren. Dabei werden auch Verantwortlichkeiten und ein Zeitplan für die Implementierung der Maßnahmen festgelegt. Die in der vierten Phase durchgeführte Kategorisierung der Risiken nach Folgenschwere und deren Eintrittswahrscheinlichkeit gibt vor, welche Maßnahmen priorisiert werden sollten. Jedenfalls sollte der Action Plan aber sämtliche identifizierten Risiken abdecken. Das gilt auch dann, wenn die Organisation entscheidet, sie zunächst oder dauerhaft zu tolerieren.[46]

f) Sechste Phase

Die sechste Phase kann mit der Erstellung eines DSFA-Berichts beginnen, in dem sämtliche vorherigen Phasen dokumentiert werden. Abhängig von der Hierarchiestruktur des Unternehmens, das die DSFA durchführt, kann eine Genehmigung des Berichts und des darin enthaltenen Action Plans notwendig sein. Im Anschluss werden die vorgesehenen Maßnahmen implementiert.[47]

4. Auftragsverarbeitung

Während die DS-GVO ausführliche Vorschriften zur Auftragsverarbeitung enthält, allen voran Art. 28 und 29 DS-GVO, sind die Vorschriften des PDPA (auch) in diesem Bereich knappgehalten. Nach Art. 2 Abs. 1 PDPA ist ein Auftragsverarbeiter (Data Intermediary) eine Organisation, die personenbezogene Daten im Auftrag einer anderen Organisation, des Data Controller[48], verarbeitet. Art. 4 Abs. 2 PDPA stellt fest, dass die Hauptpflichten des PDPA nur eingeschränkt für Data Intermediaries gelten, die auf Grund eines schriftlichen Vertrags für den Data Control-

28 S. hierzu PDPC, Guide to Data Protection Impact Assessments, Stand: 14.9.2021, S. 31.
29 PDPC, Guide to Data Protection Impact Assessments, Stand: 14.9.2021, S. 13.
30 PDPC, Guide to Data Protection Impact Assessments, Stand: 14.9.2021, S. 17.
31 So auch ersichtlich aus einem von der PDPC illustrierten Fallbeispiel, PDPC, Guide to Data Protection Impact Assessments, Stand: 14.9.2021, S. 14 ff.
32 PDPC, Guide to Data Protection Impact Assessments, Stand: 14.9.2021, S. 18.
33 Ein detaillierter Beispiel-Fragebogen findet sich in PDPC, Guide to Data Protection Impact Assessments, Stand: 14.9.2021, S. 33 f.
34 Vgl. Sec. 13 PDPA.
35 Vgl. Sec. 20 PDPA.
36 Vgl. Sec. 18 PDPA.
37 Vgl. Sec. 23 PDPA.
38 Vgl. Sec. 21 ff. PDPA.
39 Vgl. Sec. 24 PDPA.
40 Vgl. Sec. 25 PDPA.
41 Vgl. Sec. 26 PDPA; ausführlicher zur Übermittlung personenbezogener Daten an Empfänger in einem Drittland Blasius ZD 2021, 145 (149 f.).
42 Vgl. Sec. 26A ff. PDPA.
43 Vgl. Sec. 12 lit. a–c PDPA.
44 PDPC, Guide to Data Protection Impact Assessments, Stand: 14.9.2021, S. 18.
45 Vgl. PDPC, Guide to Data Protection Impact Assessments, Stand: 14.9.2021, S. 31.
46 PDPC, Guide to Data Protection Impact Assessments, Stand: 14.9.2021, S. 26.
47 PDPC, Guide to Data Protection Impact Assessments, Stand: 14.9.2021, S. 29.
48 Den im Gesetz nicht vorkommenden Begriff verwendet die Kommission etwa in PDPC, Guide to Managing Data Intermediaries, Stand: 2020, abrufbar unter: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Managing-Data-Intermediaries--2020.pdf, S. 5.

ler tätig werden. Mit Bezug auf die im Auftrag des Data Controller durchgeführte Datenverarbeitung finden für sie lediglich die Protection Obligation (Sec. 24 PDPA), die Retention Limitation Obligation (Sec. 25 PDPA) und – eingeschränkt – die Data Breach Notification Obligation (Sec. 26C Abs. 3 lit. a, 26E PDPA) Anwendung. Dagegen hat der Data Controller in Bezug auf personenbezogene Daten, die in seinem Auftrag und für seine Zwecke verarbeitet werden, die gleichen Pflichten, als hätte er die personenbezogenen Daten selbst verarbeitet, Sec. 4 Abs. 3 PDPA.

Die Regeln der Auftragsverarbeitung erschließen sich Unternehmen idR nicht intuitiv und werden daher regelmäßig missachtet. Aus Praktikersicht lässt sich ein Scheitern häufig bereits bei der fundamentalen Aufgabe dokumentieren, Bereiche mit bestehenden Auftragsverarbeitungsverhältnissen zu identifizieren. Sowohl im IT-Bereich, etwa bei der Nutzung eines Cloudspeicher-Anbieters, als auch bei traditionell ausgelagerten Unternehmensdienstleistungen, wie zB der Lohnbuchhaltung, fehlt den Verantwortlichen vielmals das Bewusstsein, den Vorgang datenschutzrechtlich korrekt einzuordnen. Und selbst wenn das Bestehen eines Auftragsverarbeitungsverhältnisses erkannt wurde, wird dieses in vielen Fällen nicht so gehandhabt, wie es die Verpflichtung, personenbezogene Daten angemessen zu schützen (Protection Obligation, Sec. 24 PDPA), erfordern würde.

Wie eine optimale Behandlung von Auftragsverarbeitungsverhältnissen aus Sicht der PDPC aussieht, hat die Kommission in ihrem Guide to Managing Data Intermediaries (DI Guide)[49] zusammengefasst. Sie unterscheidet hierbei zwischen vier Phasen.

a) Erste Phase
In der ersten Phase findet eine Auseinandersetzung mit den mit der Auftragsverarbeitung verfolgten Zielen, mit der Menge und Sensitivität der betroffenen personenbezogenen Daten und mit den Risiken, die mit der Auftragsverarbeitung verbunden sind, statt. Darauf basierend können Anforderungen herausgearbeitet werden, die ggf. im Auftragsverarbeitungsvertrag mit dem Data Intermediary festgelegt werden müssen. Außerdem können Auswahlkriterien zur Evaluierung und Auswahl eines geeigneten Auftragsverarbeiters aufgestellt werden.[50] Data Intermediaries sollten vor allem anhand der folgenden Faktoren bewertet und ausgewählt werden:

- der allgemeinen Fähigkeit, datenschutzrechtliche Verpflichtungen zu erfüllen und personenbezogene Daten angemessen zu behandeln,
- ihrer allgemeinen datenschutzrechtlichen Struktur, inklusive ihrer Richtlinien und Prozesse (insbesondere auch mit Blick auf datenschutzrechtliche Schulungen der Belegschaft) und
- der Maßnahmen, die sie zum Schutz personenbezogener Daten implementieren.[51]

Die Ausführungen im DI Guide erinnern insoweit an Art. 28 Abs. 1 DS-GVO. Anders als Art. 28 Abs. 3 DS-GVO schreibt der PDPA nicht ausdrücklich vor, dass ein Auftragsverarbeitungsvertrag abgeschlossen werden muss und welchen Mindestinhalt dieser zu haben hat. Für die PDPC ergibt sich die Notwendigkeit eines solchen Data Processing Agreement allerdings aus einer Interpretation der Protection Obligation. Diese verletzt der Data Controller, wenn weder ein Vertrag noch ein anderes äquivalentes Dokument existiert, in dem die Pflichten und Verantwortlichkeiten der Parteien definiert werden und insbesondere Folgendes festgehalten wird:

- der Umfang der ausgelagerten Datenverarbeitung,
- die datenschutzrechtlichen Anforderungen an den Auftragsverarbeiter und
- die Plichten und Verantwortlichkeiten der Parteien hinsichtlich der Datenverarbeitung.[52]

Weitere Erwägungen zu möglichen Vertragspunkten hält die PDPC in Annex B ihres DI Guide fest.

b) Zweite Phase
Die vertragliche Einigung der Parteien bildet den Ausgangspunkt der zweiten Phase der Auftragsverarbeitung. Abhängig vom Umfang der konkreten Verarbeitung sollte sie durch die Festlegung von Standard Operating Procedures ergänzt werden.[53]

c) Dritte Phase
Die dritte Phase gilt der Durchführung und Überwachung der Auftragsverarbeitung. Hierzu können – je nach Komplexität des Projekts – insbesondere folgende Maßnahmen gehören:

- Gespräche und Treffen mit dem Auftragsverarbeiter,
- Schulungen der Mitarbeiter des Auftragsverarbeiters,
- Audits und Inspektionen vor Ort,
- periodische Berichte sowie
- Planspiele und Table-Top Exercises.[54]

d) Vierte Phase
In der vierten und letzten Phase sollte ein bereits im Vorfeld bestimmter Exit Management Plan umgesetzt werden. Der Plan soll klare Vorgaben dazu enthalten, wann und ggf. wie der Auftragsverarbeiter sich der verarbeiteten personenbezogenen Daten zu entledigen hat. Er kann außerdem die Dokumentation des Gesamtprojekts durch den Auftragsverarbeiter sowie Abschlussprüfungen durch den Data Controller vorsehen.[55]

III. Fazit

Während der gesetzliche Pflichtenkatalog des PDPA bedeutend kürzer gehalten ist als derjenige der DS-GVO, führen die Leitfäden der PDPC oft zu ähnlichen Anforderungen. Der Rückgriff auf bekannte Konzepte kann so insbesondere lokalen Gruppengesellschaften deutscher Konzerne die Basis-Compliance erleichtern.

Sind die notwendigen Grundlagen geschaffen, sollten Organisationen darauf achten, auch die übrigen Pflichten des PDPA zu erfüllen. Dazu gehören die unter II.3. angesprochenen Main Obligations, also etwa die Transfer Limitation Obligation, die Regeln für die Übermittlung personenbezogener Daten ins Ausland aufstellt.[56] Auch diese Main Obligations sind in ähnlicher Weise aus der DS-GVO bekannt.

So verlockend dies auch sein mag, lässt sich aus aller Vergleichbarkeit dennoch nicht der Schluss ziehen, dass die Einhaltung der Vorschriften der DS-GVO zwingend auch zur Einhaltung der Regeln des PDPA führt. Denn teilweise sind die Anforderungen des PDPA strikter als die des europäischen Pendants. Die datenschutzrechtliche Strategie eines Unternehmens sollte sich daher immer an den Notwendigkeiten des lokalen Rechts ausrichten.

49 PDPC, Guide to Managing Data Intermediaries, Stand: 2020.
50 PDPC, Guide to Managing Data Intermediaries, Stand: 2020, S. 10.
51 PDPC, Guide to Managing Data Intermediaries, Stand: 2020, S. 12.
52 PDPC, Guide to Managing Data Intermediaries, Stand: 2020, S. 13 f.; PDPC, [2019] SGPDPC 3, 18, abrufbar unter: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Grounds-of-Decision---SingHealth-IHiS---150119.pdf.
53 PDPC, Guide to Managing Data Intermediaries, Stand: 2020, S. 16 ff.
54 PDPC, Guide to Managing Data Intermediaries, Stand: 2020, S. 20 ff.
55 PDPC, Guide to Managing Data Intermediaries, Stand: 2020, S. 26.
56 Nur der Vollständigkeit halber sei erwähnt, dass der PDPA bei einer Übermittlung von personenbezogenen Daten aus einem Drittstaat nach Singapur keine Anforderungen vorsieht, die über diejenigen hinausgehen, die auch bei rein landesinternen Sachverhalten gelten.

Schnell gelesen ...

- Auf Grund der knappen Regelungen des singapurischen Datenschutzgesetzes vernachlässigen Organisationen regelmäßig grundlegende Compliance-Anforderungen. Das betrifft insbesondere Bereiche wie die Bestellung eines Datenschutzbeauftragten, das Führen eines Verzeichnisses von Verarbeitungstätigkeiten, die Durchführung von Datenschutz-Folgenabschätzungen und die Auftragsverarbeitung.
- Während Unternehmen mit deutschen Wurzeln in dieser Hinsicht häufig von einer Ähnlichkeit zwischen singapurischen und europäischen Anforderungen profitieren, sind die lokalen Vorgaben unbedingt zu beachten.
- Die Vorgaben ergeben sich häufig aus Leitfäden der singapurischen Datenschutzkommission.

Sebastian Blasius ist als Rechtsanwalt in Singapur tätig.
Sebastian.Blasius@Gateway-Law.com
+6589028272
https://gateway-law.com/sebastian-blasius-german/