Globale Auswirkungen von Datenschutz-vorschriften

Der Datenschutz prägt Branchen weltweit

«Ich glaube wirklich, dass wir keinen Kompromiss zwischen Sicherheit und Datenschutz machen müssen. Ich bin der Ansicht, dass es uns die Technologie ermöglicht, beides zu haben.»

John Poindexter

pwc

Inhalt

Schutz personenbezogener Daten – Einleitung

Die Welt durchlebt gerade ihre vierte industrielle Revolution, welche von extremen sozialen und wirtschaftlichen Verflechtungen geprägt ist. Eine Revolution, die auch von der Digitalisierung und die Datenverfügbarkeit genährt wurde und – wenn man die Tag für Tag exponentiell zunehmende Menge verarbeiteter Informationen in Betracht zieht – immer noch wird. Die meisten Tätigkeiten erzeugen in irgendeiner Form Daten: von einem einfachen Telefongespräch bis hin zu weniger offensichtlichen Beispielen wie dem Kauf von Lebensmitteln mit einer Kredit- oder Kundenkarte. Diese beständig wachsende Datenmenge muss von Unternehmen gespeichert und verwaltet werden, wobei diese wiederum selbst komplexer werden müssen, um in der modernen, digitalisierten Welt zu überleben.

Angesichts ihrer Bedeutung steht die Verarbeitung personenbezogener Daten heute ganz oben auf der Agenda vieler Staaten weltweit. Die EU setzte mit der Veröffentlichung der Datenschutz-Grundverordnung (DSGVO) einen regulatorischen Standard und hat damit eine Messlatte für die Aktualisierung und Überprüfung der meisten weltweiten Datenschutzgesetze gelegt. Mit Inkrafttreten der DSGVO müssen Unternehmen weltweit mit einer Welle neuer oder aktualisierter Vorschriften rechnen und darauf vorbereitet sein, immer striktere Anforderungen erfüllen zu müssen. In diesem Dokument beschreiben wir ausführlich, wie sich bestimmte Vorschriften ändern und was Unternehmen bei der Verarbeitung personenbezogener Daten beachten müssen, um in diesem stark regulierten Umfeld zu bestehen.

Darum ist Datenschutz wichtig

Heutzutage verwalten Menschen ihre personenbezogenen Daten in einer Weise, die noch vor wenigen Jahrzehnten undenkbar gewesen wäre. Hätte in den 1980er-Jahren jemand seine Adresse, Telefonnummer und sein Jahreseinkommen einer völlig fremden Person gegenüber offengelegt, der er im Bus begegnete? Wohl kaum. Heute jedoch teilen die Menschen eine unvorstellbare Menge an Daten mit Unternehmen – im Wesentlichen völlig Fremden – und meist deswegen, weil wir alle darauf vertrauen, dass unsere Daten rechtmässig und im Einklang mit den Grundprinzipien des Datenschutzes verarbeitet werden. Wir gehen davon aus, dass unsere Daten sicher und vertraulich behandelt werden, dass kein Dritter darauf zugreifen kann und dass das Unternehmen, dem wir unsere Daten anvertraut haben, sie nur zu den Zwecken nutzt, zu denen wir sie offengelegt haben. Wir haben dieses Vertrauen, weil strenge Datenschutzvorschriften gelten und Unternehmen ein Interesse daran haben, sicherzustellen, dass unsere Daten weiterhin geschützt sind.

Trotz aller Bemühungen funktioniert das jedoch nicht immer, wie der jüngste Datenskandal im Zusammenhang mit Facebook und Cambridge Analytica belegt: Millionen personenbezogener Datenprofile auf Facebook wurden mutmasslich ohne Genehmigung analysiert und für illegale politische Zwecke genutzt. Solche Fälle unterstreichen die Notwendigkeit schärferer und transparenterer Vorschriften – wie der EU-DSGVO, die im Mai 2018 nach den Ereignissen in Verbindung mit dem Missbrauchskandal von Cambridge Analytica in Kraft trat.

Meilenstein des Datenschutzes: EU-DSGVO

Die Forderung nach der neuen Datenschutz-Grundverordnung der Europäischen Union (EU-DSGVO) entstand aus dem Bedürfnis nach strengeren gesetzlichen Anforderungen beim Schutz personenbezogener Daten. Die DSGVO musste einen viel grösseren Anforderungsbereich als die 1995 verabschiedete Vorgänger-Richtlinie 65/46/EU abdecken. Die DSGVO wurde am

24. Mai 2016 mit einem Umsetzungszeitraum von zwei Jahren bis Mai 2018 (Datum des Inkrafttretens) veröffentlicht. Es handelte sich dabei um ein neues Regelwerk, das Privatsphäre und Datenschutz aller EU-Bürger in der Union und im Ausland stärken soll.

Alle Unternehmen, unabhängig von ihrem geografischen Standort, die personenbezogene Daten von EU-Bürgern erheben oder verarbeiten, müssen die DSGVO erfüllen. Dazu zählen auch Unternehmen ohne Geschäftsräume in der EU, die aber Waren und Dienstleistungen in der EU anbieten oder EU-Bürger überwachen. Befolgen derartige Unternehmen die DSGVO nicht, hat das erhebliche finanzielle Konsequenzen. Die Geldbussen betragen bis zu vier Prozent des weltweiten Jahresgesamtumsatzes oder 20 Millionen Euro – je nachdem, welcher Betrag höher ist.

Die DSGVO wird von vielen als Meilenstein im Datenschutz gelobt, da sie ein noch nie dagewesenes Schutzniveau der betroffenen Person vorsieht. Sie legt nicht nur strenge Grundsätze bei der Verarbeitung personenbezogener Daten fest, sondern gewährt betroffenen Personen auch eine Reihe an Rechten, die ihnen mehr Kontrolle darüber verleihen, wie ihre personenbezogenen Daten verarbeitet werden. Das bemerkenswerteste dieser Rechte ist eindeutig das Recht, vergessen zu werden: In einer digitalisierten Welt, in der alle Daten dazu bestimmt zu sein scheinen, für immer auf irgendeinem Server gespeichert zu werden, gewährt dieses Recht betroffenen Personen die Möglichkeit, die Löschung ihrer Daten zu verlangen, wenn diese nicht länger für den Zweck, zu dem sie erfasst wurden, benötigt werden. Insbesondere müssen Unternehmen über die Möglichkeit verfügen, auf Antrag Daten von all ihren Systemen zu löschen (einschliesslich der Systeme anderer Unternehmen, an die Daten übertragen wurden).

Der Compliance-Rahmen der EU-DSGVO

Die EU-DSGVO beinhaltet acht wichtige Aspekte, die aus drei unterschiedlichen Perspektiven operativ abgedeckt werden müssen: Geschäft (Art der Datenverarbeitung), IT (Ort der Datenverarbeitung) und Dritte (Empfänger der personenbezogenen Daten).

1

Datenbestand
Organisationen müssen einen Datenbestand aufbauen und pflegen, um ermitteln zu können, welche personenbezogenen Daten zu welchem Zweck verarbeitet werden.

2

Grundsätze
Bei der Verarbeitung personenbezogener Daten müssen immer die Grundsätze des Schutzes personenbezogener Daten beachtet werden (d.h. sie muss gesetzeskonform sein, einem bestimmten Zweck dienen usw.).

3

Standards
Um sicherzustellen, dass personenbezogene Daten die DSGVO-Anforderungen erfüllen, müssen die Unternehmen entsprechende Prozesse erarbeiten und Verhaltensstandards durchsetzen.

4

Rechte von betroffenen Personen
Die DSGVO gewährt natürlichen Personen mehrere Rechte (Rechte von betroffenen Personen), die Organisationen beachten müssen (z.B. Datenzugangsrecht oder Recht auf Vergessenwerden).

5

Verzeichnis über Datenverarbeitungstätigkeiten
Die Verordnung sieht vor, dass Organisationen ein detailliertes Verzeichnis über alle Tätigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten führen müssen.

6

Verletzungen des Schutzes personenbezogener Daten
Unternehmen müssen das Risiko von Verletzungen des Datenschutzes minimieren und Prozesse umsetzen, die sicherstellen, dass die Aufsichtsbehörde innerhalb von 72 Stunden informiert wird (wenn bestimmte Voraussetzungen erfüllt sind).

7

Datenschutzbeauftragter
Unter bestimmten Voraussetzungen müssen Organisationen einen Datenschutzbeauftragten ernennen, um die DSGVO-Anforderungen zu erfüllen.

8

Datenschutzfolgenabschätzung
Für Verarbeitungstätigkeiten, die ein Risiko für die Rechte und die Freiheit von Personen bergen, muss eine Folgenabschätzung durchgeführt werden, um geeignete Korrekturmassnahmen umsetzen zu können.

Aktueller Stand der DSGVO-Umsetzung

Die Sicherstellung der DSGVO-Compliance erfordert von den Unternehmen in Europa und dem Rest der Welt massive Investitionen. Einige Unternehmen können der neuen Regulierung jedoch auch gute Seiten abgewinnen. Die Einhaltung der Vorschrift hat Unternehmen, die bereits konsequent ihren Datenschutzansatz neu definiert hatten, auch neue Chancen geboten, die es ihnen letztlich ermöglichen, vom Wert der Daten, die sie besitzen, zu profitieren. Sie waren in der Lage, ein Setup zu entwickeln, das besser geeignet ist, in der neuen digitalen Wirtschaft das Vertrauen der betroffenen Personen zu gewinnen, indem ihnen mehr Transparenz und Kontrolle über ihre eigenen Daten gewährt wird.

Viele Unternehmen in der EU und in anderen Ländern wie der Schweiz haben einen risikobasierten Ansatz für die Umsetzung der Massnahmen zur Einhaltung der DSGVO gewählt. Dieser Ansatz sieht vor, dass bestimmten Massnahmen gegenüber anderen Vorrang verliehen wird. Einige Unternehmen schlossen die Umsetzung ihrer Compliance-Vorkehrungen mit dem Inkrafttreten der DSGVO im Mai 2018 ab. Die meisten allerdings sind noch mit einem oder mehreren der nachfolgenden Schritte beschäftigt:

1. Sicherstellung der Wirksamkeit der umgesetzten Massnahmen. Dies ist insbesondere in Bezug auf die Verfahren im Zusammenhang mit der Erfassung personenbezogener Daten und Verletzungen des Schutzes personenbezogener Daten wichtig
2. Automatisierung der implementierten Prozesse, wo möglich, um die Compliance-Kosten zu senken. Viele Unternehmen haben aufwendige manuelle Prozesse implementiert, die jedoch langfristig oft automatisiert werden können (z.B. in Bezug auf Rechte betroffener Personen, wo die Erstellung von Berichten über die persönlichen Daten von betroffenen Personen leicht automatisiert werden kann)
3. Überprüfung der Datenschutzbemühungen aus strategischer Sicht durch Integration der Datenverwaltung in die strategische Ausrichtung des Unternehmens. Angesichts der bereits unternommenen Anstrengungen zur Erstellung des Datenbestands ist der nächste logische Schritt die Sicherstellung, dass diese Informationen strategisch genutzt werden. Dazu sind die Daten, die Unternehmen bereits besitzen und verarbeiten, bestmöglich zu nutzen (wobei stets die Einhaltung der Datenschutzgrundsätze insbesondere im Zusammenhang mit der Zweckbindung zu berücksichtigen ist).

Wichtige Datenschutzgesetze in Europa und weltweit

Der Datenschutz hat sich in vielen Ländern weltweit zu einem brisanten Thema entwickelt. Ob Ihr Unternehmen in Europa oder einer entlegenen Region Chinas ansässig ist: Sie werden in irgendeiner Form mit Vorschriften zum Schutz personenbezogener Daten konfrontiert werden – für Unternehmen mit globaler Präsenz eine oftmals sehr komplexe Angelegenheit. Und zwar derart, dass es für ein Unternehmen mit Sitz in den USA effizienter sein kann, einfach an allen Standorten, an denen es tätig ist, die europäische DSGVO zu befolgen – denn die meisten anderen Vorschriften sind in der Regel gleichwertig oder weniger streng als die DSGVO.

In diesem Abschnitt möchten wir Ihnen einen ausführlichen Überblick über die zentralen Datenschutzvorschriften in einigen der wichtigsten Regionen weltweit geben.

EU: lokale Abweichungen von der DSGVO

Die DSGVO ist eine Vorschrift und als solche gilt sie automatisch in allen EU-Mitgliedstaaten, ohne dass sie in nationale Gesetze umgesetzt werden muss. Die Staaten können jedoch immer noch in einigen Bereichen der Vorschrift ein gewisses Ermessen walten lassen. Tatsächlich lässt der Text in bestimmten Abschnitten nationale Abweichungen zu (z.B. Verarbeitung spezieller Kategorien personenbezogener Daten oder Datenübertragungen).

In der Praxis können nationale Gesetze, wo die DSGVO Abweichungen zulässt, in bestimmten Bereichen mehr oder weniger streng als die DSGVO sein. Im Folgenden einige Beispiele für Unterschiede bei den grössten europäischen Ländern. Der volle Umfang der Abweichungen ist jedoch zu gross, um hier abgedeckt zu werden. Wir raten Unternehmen daher, eine umfassende Analyse der veröffentlichten nationalen Abweichungen in den Ländern vorzunehmen, in denen sie tätig sind.

Land	Abweichung von der DSGVO
Vereinigtes Königreich	Angesichts des nahenden Brexit wird das britische Datenschutzgesetz genauestens überwacht, da es die Richtung zu einem britischer geprägten Datenschutzgesetz weisen kann (insoweit die DSGVO nicht mehr direkt anwendbar ist). Der Data Protection Act, der seit Mai 2018 gilt, enthält zahlreiche Abweichungen von der DSGVO, wovon hier die nennenswertesten: • Die britischen Abweichungen sehen strengere Bedingungen für die Verarbeitung spezieller Kategorien personenbezogener Daten vor (wie biometrische Angaben oder Daten zur sexuellen Orientierung), bei denen eine ausdrückliche Einwilligung erforderlich ist. Die Verarbeitung dieser speziellen Kategorien personenbezogener Daten muss besondere Bedingungen erfüllen, um als rechtmässig zu gelten. • Der britische Data Protection Act verlangt auch, dass geeignete Sicherheitsvorkehrungen und Richtlinien für die Verarbeitung spezieller Kategorien personenbezogener Daten vorhanden sind und diese in Form von Verzeichnissen angemessen dokumentiert werden (vgl. Art. 30 DSGVO).
Deutschland	In Deutschland trat das neue Bundesdatenschutzgesetz (BDSG) im Mai 2018 in Kraft. Es enthält zusätzliche, strengere Anforderungen für die Verarbeitung personenbezogener Daten. • So gelten spezielle Anforderungen für die Verarbeitung von Videoaufnahmen: Unternehmen müssen nicht nur sicherstellen, dass diese Tätigkeit die Rechte und Freiheiten von Personen nicht gefährdet, sondern eine derartige Verarbeitung ist auch nur dann zulässig, wenn bestimmte Bedingungen erfüllt werden. Angesichts des weitverbreiteten Einsatzes von Videoüberwachungsanlagen wird dies eine der am schwierigsten zu erfüllenden Anforderungen sein.

Land	Abweichung von der DSGVO
	• Wo die DSGVO die Risikominderung für die betroffenen Personen im Rahmen einer automatisierten Entscheidung einschliesslich Profiling verlangt, ist nach den deutschen Vorschriften die Verarbeitung personenbezogener Daten für Scoring-Zwecke nur unter bestimmten Bedingungen zulässig.
Österreich	Die österreichischen Abweichungen (aufgelistet im aktualisierten Datenschutzgesetz von 2018) sind vom Umfang her beschränkt, aber meist strenger als die jeweiligen Anforderungen in der DSGVO. Hier einige Beispiele: • Wie in Deutschland gibt es besondere Anforderungen bei der Verarbeitung von Videoaufzeichnungen. Auch hier ist die Verarbeitung nur unter bestimmten Bedingungen zulässig. • Wo sich die DSGVO nur auf die Pflichten der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter als juristische Personen konzentriert, stellt das österreichische Datenschutzgesetz besondere Anforderungen an die Mitarbeitenden dieser Unternehmen, die haftbar sind, sollten sie im Rahmen ihrer Beschäftigung verarbeitete personenbezogene Daten nicht vertraulich behandeln.
Frankreich	Das überarbeitete französische Datenschutzgesetz (in Kraft seit Mai 2018) stellt eine Reihe Anforderungen, die teils strenger als die entsprechenden Artikel der DSGVO sind. Beispiele: • Das französische Gesetz verbietet ausdrücklich die Verarbeitung spezieller Kategorien personenbezogener Daten, sofern die in der Abweichung genannten Bedingungen nicht erfüllt sind. Diese Vorschrift ist vorrangig an die DSGVO-Vorgabe angepasst, aber hinsichtlich der Verarbeitung biometrischer Informationen im Rahmen der Beschäftigung strenger. • Die DSGVO sieht bei Kindern ein Mindestalter von 16 Jahren vor, um in Angebote von Online-Diensten einwilligen zu können. Das französische Gesetz setzt das Mindestalter auf 15 Jahre herunter (bei zusätzlichen lokalen Anforderungen).
Italien	Italien veröffentlichte im September 2018 – mit einigen Monaten Verspätung gegenüber anderen europäischen Ländern – lediglich eine überarbeitete Version ihrer Datenschutzbestimmungen. Nennenswert sind folgende Regelungen: • Das italienische Gesetz sieht härtere Strafbestimmungen vor, wenn personenbezogene Daten widerrechtlich verarbeitet werden. • Auch in Italien wurde das Mindestalter für die Einwilligung von Kindern in Angebote von Online-Diensten herabgesetzt – und zwar auf 14 Jahre.

Datenschutz weltweit

Während die EU-DSGVO bereits in Kraft ist, haben andere Länder erst mit der Arbeit an ihren eigenen Datenschutzgesetzen begonnen – und versuchen dabei oft, sie an die Anforderungen der DSGVO anzugleichen. Im Folgenden ein Überblick, inwiefern andere, derzeit in der Überprüfung befindliche Datenschutzgesetze der DSGVO entsprechen, daneben eine ausführlichere Beschreibung des aktuellen Gesetzesstatus in den jeweiligen Ländern.

Land	Wichtigste Datenschutz-bestimmung	Neues oder aktualisiertes Gesetz	Vergleichbarkeit mit der DSGVO	Zeitplan
Schweiz	Bundesgesetz über den Datenschutz	Aktualisiert	Hohe Vergleichbarkeit	Voraussichtlich Ende 2020 vollumfänglich in Kraft
USA	Je nach Bundesstaat unterschiedlich	Neu und aktualisiert	Je nach Bundesstaat unterschiedlich	k.A.
Kanada	Digital Privacy Act	Aktualisiert	Entsprechend den DSGVO-Anforderungen aktualisiert	Voraussichtlich Ende 2019 in Kraft
China	Chinese National Standards on Information Security Technology – Personal Information Security Specification	Neu	Einige Anforderungen sind sogar strenger als die DSGVO	Im Mai 2018 in Kraft getreten
Indien	Entwurf Datenschutzgesetz	Neu (Entwurf)	Beim derzeitigen Stand im Vergleich zur DSGVO geringerer Schutz personen-bezogener Daten	Der Entwurf wurde im Juli 2018 vorgelegt.
Thailand	Entwurf Datenschutzgesetz	Neu (Entwurf)	Soll der DSGVO entsprechen	Der Entwurf wurde im Mai 2018 genehmigt
Singapur	Gesetz zum Schutz personen-bezogener Daten	Vorhanden (keine Veränderungen)	Vergleichbares Schutzniveau wie DSGVO	k.A.
Jersey	Datenschutzgesetz	Aktualisiert	Folgt Anforderungen der DSGVO	Im Mai 2018 in Kraft getreten

Datenschutz in der Schweiz: DSG

Am 9. Dezember 2011 genehmigte der Bundesrat den Bericht über die Evaluation des Bundesgesetzes über den Datenschutz und wies das Eidgenössische Justiz- und Polizeidepartement (EJPD) an, gesetzgeberische Massnahmen zur Stärkung des Datenschutzes zu prüfen mit Blick auf die Ergebnisse der Evaluation und die aktuellen Entwicklungen in der EU und im Europarat. Darüber hinaus war die Überarbeitung vorhandener Gesetze aufgrund des Schengen-Abkommens erforderlich.

Die Anpassung des DSG an die DSGVO ist aus wirtschaftlicher Sicht unabdingbar, da der Datenaustausch mit Unternehmen und staatlichen Behörden aus Ländern, die nicht über einen vergleichbaren Schutz personenbezogener Daten verfügen, nur unter erschwerten Bedingungen erfolgen kann (unterschiedliche Anforderungsniveaus für das gleiche Unternehmen, Beschränkung der Geschäftstätigkeit mit bestimmten Unternehmen usw.).

Im September 2017 legte der Bundesrat einen Entwurf für ein gründlich überarbeitetes Datenschutzgesetz – das Bundesgesetz über den Datenschutz (DSG) – vor, das folgende Ziele hat: (i) höhere Transparenz (z.B. müssen für die Verarbeitung Verantwortliche durch geeignete Voreinstellungen gewährleisten, dass standardmässig nur personenbezogene Daten verarbeitet werden, die für den jeweiligen Zweck erforderlich sind); (ii) mehr Mitbestimmungsrechte betroffener Personen (z.B. müssen für die Verarbeitung Verantwortliche den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten so bald wie möglich über einen Verstoss gegen den Datenschutz informieren, wenn ein hohes Risiko für die Persönlichkeits- oder Grundrechte der betroffenen Person besteht); (iii) und Berücksichtigung des technologischen Fortschritts (so wurde auch genetischen und biometrischen Daten, die eine natürliche Person eindeutig identifizieren, Rechnung getragen).

Die Revision erfolgt in zwei Phasen. Die erste sieht – gemäss den Anforderungen des Schengen-Abkommens – eine vorherige Konsultation bezüglich der Umsetzung des EU-Gesetzes (Richtlinie 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Rahmen der Strafverfolgung) vor. Anschliessend kann das Datenschutzgesetz ohne Zeitdruck überarbeitet werden. Die zweite Phase, die voraussichtlich Ende 2020 abgeschlossen ist, ist besonders für Schweizer Unternehmen relevant. Weitere und ausführlichere Informationen zum DSG und seiner Verknüpfung mit der DSGVO finden sich in unserer Publikation «Was bringt die Revision des Schweizer Datenschutzgesetzes mit sich, und wie hängt dies mit der DSGVO und der ePrivacy-Verordnung zusammen?»

Datenschutz in den USA

Die USA verfügen auf Bundesebene über 20 branchenspezifische Datenschutzgesetze. Darüber hinaus gibt es Hunderte bundesstaatlicher Gesetze, die die Erhebung und Nutzung personenbezogener Daten regeln – und ihre Anzahl steigt von Jahr zu Jahr. In einigen Fällen haben Bundesgesetze Vorrang vor bundesstaatlichen Datenschutzgesetzen zum gleichen Thema. So hat zum Beispiel das Bundesgesetz über kommerzielle E-Mails und das Teilen von E-Mail-Adressen Vorrang vor den meisten bundesstaatlichen Gesetzen, die ebenfalls den Umgang mit solchen Daten regeln. Aber nicht alle Bundesdatenschutzgesetze haben automatisch Vorrang vor bundesstaatlichen Vorschriften. Somit kann ein Unternehmen in Situationen geraten, in denen es unterschiedliche Bundes- und bundesstaatliche Gesetze beachten muss, welche die gleichen Datenarten regulieren, wie etwa medizinische oder Gesundheitsdaten.

Die meisten Staaten verfügen heute über irgendeine Form von Datenschutzgesetzgebung, Kalifornien ist in dieser Hinsicht jedoch führend. Der Bundesstaat hat eine Vielzahl von Datenschutzgesetzen umgesetzt, wobei einige weitreichende Wirkung auf nationaler Ebene entfalten. So war Kalifornien etwa der erste Staat, der 2002 ein Gesetz über die Meldung von Sicherheitsverletzungen erliess (California Civil Code § 1798.82). Auch dem US-Kongress wurde indessen eine Reihe von Entwürfen vorgelegt, die einen nationalen Standard für die Meldung von Datenschutzverstössen setzen würden. Bis jetzt wurde jedoch noch keiner angenommen.

Datenschutz in Kanada

Kanada hat vier Datenschutzgesetze im Privatsektor, die die Erhebung, Nutzung, Offenlegung und Verwaltung personenbezogener Daten regeln: (i) den Federal Personal Information Protection and Electronic Documents Act, S.C. 2000, (PIPEDA); (ii) den Personal Information Protection Act, S.A. 2003 in Alberta (PIPA Alberta); (iii) den Personal Information Protection Act, S.B.C. 2003 in British Columbia (PIPA BC); und (iv) den Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q. in Québec (Québec Privacy Act).

Der PIPEDA, das Bundesdatenschutzgesetz, ist im Vergleich zur DSGVO weniger streng, wurde jedoch im Jahr 2018 abgeändert, um teilweise den Anforderungen der DSGVO zu entsprechen. Mit den Anforderungen des PIPEDA-Gesetzes wurden Bestimmungen zur verbindlichen Meldung von Datenschutzverletzungen eingeführt, trotzdem bleiben Schwächen im Vergleich zur DSGVO bestehen, hauptsächlich in den Bereichen Datenübertragbarkeit, Recht auf Löschung und Einwilligung.

Datenschutz in China

Die seit langem erwarteten ersten Chinese National Standards on Information Security Technology – Personal Information Security Specification GB/T 35273-2017 wurden freigegeben und sind am 1. Mai 2018 in Kraft getreten. Sie dienen als neuer De-facto-Standard für den praktischen Datenschutz, der viele bestehende Datenschutzgesetze wie etwa das Cybersicherheitsgesetz und das Verbraucherschutzgesetz ergänzt und erläutert sowie praktische Schritte zur Einhaltung beschreibt.

Wie die Standards umgesetzt werden, ist jedoch noch nicht klar. Trotz der Unsicherheit bezüglich der Umsetzung deckt der Standard weite Bereiche ab und enthält sogar strengere Anforderungen als die DSGVO. Wo sich die DSGVO beispielsweise nur auf bestimmte Datenarten konzentriert, ist der chinesische Standard in Bezug auf sensible personenbezogene Daten weitreichender. Die chinesischen Standards gelten für alle personenbezogenen Daten, die bei Verlust oder Missbrauch Schäden für Personen, Eigentum, den Ruf und die geistige und körperliche Gesundheit zur Folge hätten.

Datenschutz in Indien

Im Juli 2018 rückte Indien seinem ersten Datenschutzgesetz näher: Es wurde ein Datenschutzgesetzentwurf vorgelegt, der einen Rahmen bildet und beschreibt, wie Unternehmen einschliesslich des Staates Daten von Bürgern erheben, verarbeiten und speichern müssen. Der Entwurf weist jedoch noch viele Lücken auf, die Schutz und Sicherheit personenbezogener Daten von Bürgern schwächen können. So bringt zum Beispiel die Anforderung, eine Kopie aller personenbezogenen Daten in einem Serverzentrum in Indien zu speichern, weitreichende Ermächtigungen für die Regierung bei der Nutzung personenbezogener Daten mit sich. Daher muss der Entwurf noch mehrfach überarbeitet werden, bevor er zu einem Gesetz wird, das mit der DSGVO vergleichbar ist.

Bis dahin übernimmt der Information Technology Act von 2000 diese Rolle. Dieser enthält spezifische Vorschriften zum Schutz elektronischer Daten und regelt Aspekte wie etwa Schadenersatz. Im Übrigen sieht er erhebliche Strafen bei unerlaubter Weitergabe und Missbrauch personenbezogener Daten sowie bei einem Verstoss gegen Vertragsbestimmungen im Zusammenhang mit personenbezogenen Daten vor. Der IT Act enthält jedoch keine Bestimmungen zum Schutz und zu den anwendbaren Verfahren, um die Sicherheit sensibler personenbezogener Daten natürlicher Personen zu gewährleisten. Somit wurden einige Änderungen vorgenommen und letztlich Abschnitt 43A in den IT Act eingefügt, woraus die Information Technology Rules von 2011 entstanden. Die Datenschutzvorschriften zwingen Körperschaften, personenbezogene Daten einschliesslich sensibler personenbezogener Angaben zu erheben, verarbeiten und speichern, um bestimmten Compliance-Verfahren zu entsprechen.

Datenschutz in Thailand

Aktuell gibt es in Thailand keine spezifischen Gesetze zum Schutz personenbezogener Daten, aber das Land arbeitet seit Jahren an einer Regelung in diesem Bereich. Ein Entwurf des Personal Data Protection Act (Gesetzentwurf) wurde vom thailändischen Kabinett am 22. Mai 2018 grundsätzlich genehmigt. Eine überarbeitete Version des Dokuments wird derzeit vom Staatsrat geprüft.

Mit dem neuen Gesetzentwurf soll der Datenschutz im Land an die Mindestanforderungen vieler Datenschutzgesetze weltweit, insbesondere der DSGVO, angepasst werden. Das Gesetz muss jetzt vom Staatsrat genehmigt werden. Es wurde jedoch kein offizieller Zeitplan festgelegt, wann das neue Gesetz veröffentlicht wird und in Kraft tritt.

Datenschutz in Singapur

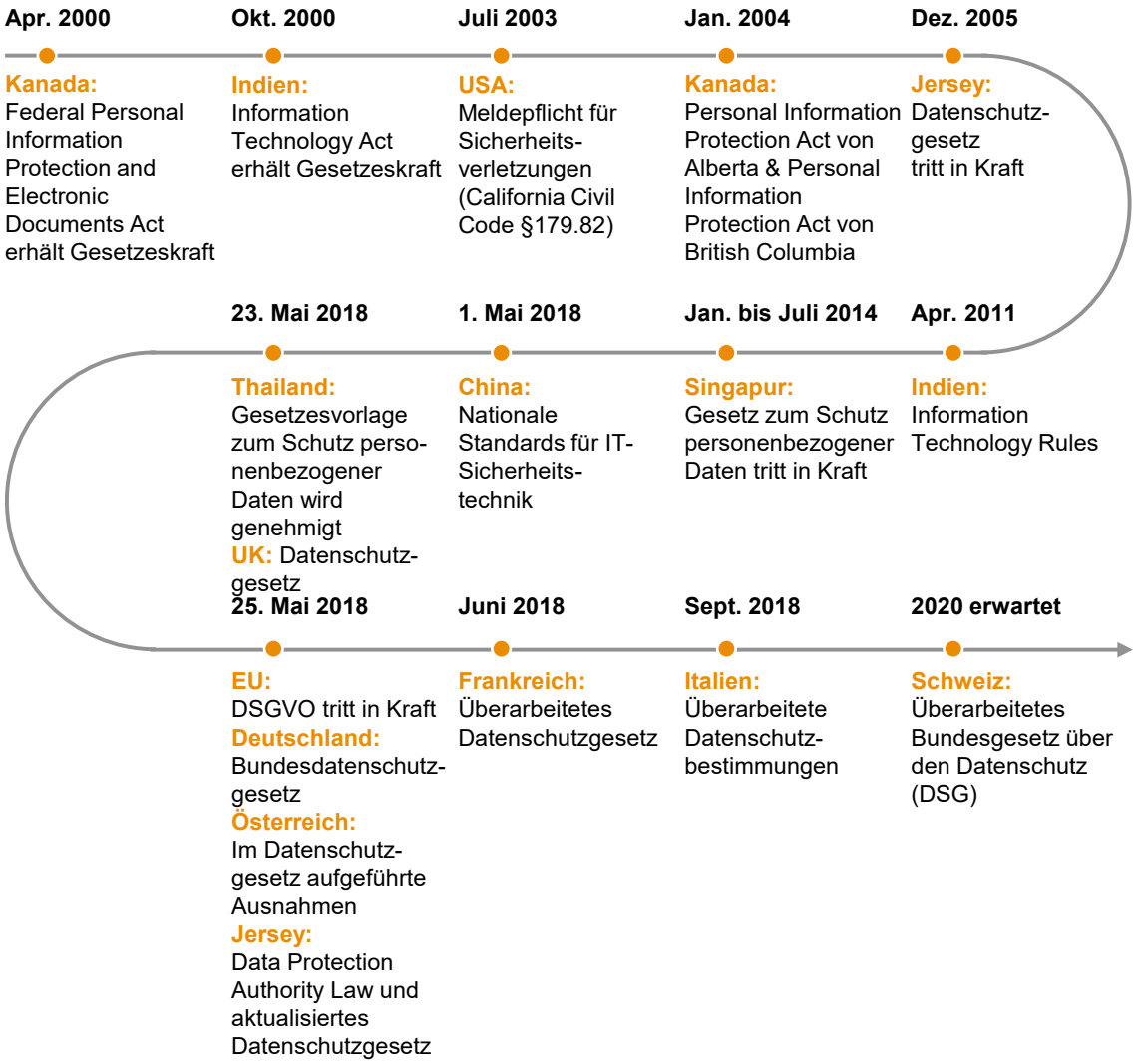
In Singapur trat der Personal Data Protection Act 2012 in Kraft und hat extraterritoriale Geltung, d.h. das Gesetz gilt für alle Unternehmen, die Daten natürlicher Personen, die im Land ansässig sind, verarbeiten – unabhängig vom Sitz des Unternehmens.

Aktuell hat Singapur eine Reihe öffentlicher Konsultationen eingeleitet, um das Gesetz in Hinblick auf wichtige Aspekte wie die Verwaltung personenbezogener Daten in der digitalen Wirtschaft oder die Verwaltung unerbetener Nachrichten und die Bereitstellung von Leitlinien zur Förderung von Innovation in der digitalen Wirtschaft zu überarbeiten.

Datenschutz in Jersey

Das Datenschutzgesetz von Jersey gilt seit 1. Dezember 2005 und basiert auf dem britischen Data Protection Act von 1998. Jersey unternimmt grosse Anstrengungen, um sicherzustellen, dass die Datenschutzvorschriften das gleiche Schutzniveau für personenbezogene Daten wie die in der EU gültigen Gesetze bieten, da historisch eine grosse Menge personenbezogener Daten, die in Jersey verarbeitet werden, zu EU-Bürgern gehören.

Das Data Protection Authority (Jersey)-Gesetz von 2018 und das Data Protection (Jersey)-Gesetz von 2018 traten in Kraft, um den erhöhten Anforderungen der DSGVO zu entsprechen. Das neue Gesetz gilt in beiden Jurisdiktionen seit dem 25. Mai 2018. Die Europäische Kommission sieht die Rechtsvorschriften zum Datenschutz in Jersey als gleichwertig zur EU-Datenschutzrichtlinie (Richtlinie 95/46/EG) an. Die Gleichwertigkeit gilt bis zur Überprüfung durch die Europäische Kommission spätestens bis 2022.



Was ist der nächste Schritt für Ihr Unternehmen?

Die DSGVO enthält einige der strengsten Anforderungen zum Datenschutz. Wie wir jedoch gesehen haben, gibt es noch eine Vielzahl anderer Datenschutzvorschriften, die Unternehmen in Europa und weltweit zu beachten haben. Auch sind viele Länder noch dabei, ihre Rechtsvorschriften zum Datenschutz zu überprüfen, aktualisieren oder zu erstellen. Auch wenn in vielen Fällen noch keine endgültige Version vorliegt (z.B. in Thailand oder der Schweiz), ist von einer hohen Vergleichbarkeit mit der EU-DSGVO auszugehen.

Datenschutz ist ein komplexes Thema. Das gilt umso mehr, wenn Ihr Unternehmen in vielen Ländern aktiv ist und damit einer Reihe unterschiedlicher Gesetze unterliegt. In diesem Fall ist genau zu prüfen, welche Vorschriften für sie gelten, wann sie handeln und welche Prozesse sie implementieren müssen. Oft ist es vermutlich leichter, ihr gesamtes Unternehmen einfach den Vorschriften der strengsten Datenschutzgesetzgebung zu unterstellen, als zu versuchen, unterschiedliche Prozesse für unterschiedliche Länder festzulegen.

Ein ganzheitlicher Ansatz stellt sicher, dass Kunden an unterschiedlichen Standorten keine Unterschiede bei den erbrachten Dienstleistungen wahrnehmen und dadurch ein kohärentes Bild entsteht – abgesehen davon, dass es oftmals der effizienteste Ansatz ist. Eine solche ganzheitliches Vorgehensweise muss nicht strikt sein: Ein risikobasierter Ansatz ist oft die beste Lösung. Zumal dieser Ansatz das Unternehmen befähigt zu erkennen, welche Lücken hinsichtlich des gesetzlichen Datenschutzes dringend geschlossen werden müssen, welche Lücken später geschlossen werden können oder welche sogar als akzeptabel für das Unternehmen hingenommen werden können. Beim Umgang mit Gesetzesentwürfen können Unternehmen, die einen risikobasierten Ansatz verfolgen, entscheiden, ob sie Implementierungsprozesse bereits auf der Grundlage der voraussichtlichen Anforderungen einleiten oder zuwarten, bis der endgültige Text vorliegt. Letzteres beinhaltet das Risiko, dass die entsprechenden Prozesse bei Inkrafttreten der Gesetze nicht implementiert sind (dies gilt insbesondere für grosse Unternehmen, die eine lange Vorlaufzeit für Transformationsprojekte benötigen, wie die Erfahrung mit der Implementierung von DSGVO-konformen Prozessen gezeigt hat).

Der Datenschutz hat heutzutage eine solche Bedeutung erlangt, dass die meisten Unternehmen es sich nicht länger leisten können, ihn einfach als weiteren Compliance-Aspekt abzutun. Eine wachsende Anzahl an Prozessen in Unternehmen umfasst auch bestimmte Formen der Verarbeitung personenbezogener Daten, und die Anforderungen aus rechtlicher Sicht werden jeden Tag strenger. Unternehmen müssen beginnen, den Schutz personenbezogener Daten aus strategischer Sicht zu betrachten. Sie müssen wissen, welche Daten sie verarbeiten und in welchen Systemen sie das tun, sie müssen angemessene Sicherheitsmassnahmen definieren und entsprechende Schulungen für die Mitarbeitenden organisieren – all dies sollte Teil der Strategie aller grossen Unternehmen werden. Ein solides Datenverwaltungssystem für die Verarbeitung personenbezogener Daten ist bei der Erfüllung aller diesbezüglichen Vorschriften ein Trumpf.

Um die Konformität in der Geschäftspraxis zu gewährleisten, sollte die Rechtslage ständig beobachtet werden, um anwendbare Gesetze zu identifizieren und zu entscheiden, wie damit aus Compliance-Sicht umgegangen werden soll. Angesichts der Bedeutung des Datenschutzes für Kunden ist es wichtig, dass entsprechende Prozesse so bald wie möglich implementiert werden. Auch Unternehmen, die der DSGVO unterliegen und bereits die entsprechenden Konformitätsprozesse implementiert haben, sollten wachsam bleiben, denn es ist mit weiteren lokalen Abweichungen zu rechnen. Zudem befindet sich eine neue Datenschutzrichtlinie für elektronische Kommunikation in Arbeit (nähere Einzelheiten finden Sie in unserer Publikation «Is ePrivacy defining the future standard of data protection for the banking industry?»).

Wie kann PwC helfen?

Als multidisziplinäre Praxisgruppe sind wir bestens positioniert, um unseren Kunden dabei zu helfen, sich an die neue Datenschutzlandschaft anzupassen. Unser Team im Bereich Datenschutz umfasst Anwälte, Berater, Cybersicherheitsspezialisten, Prüfer, Risiko- und Forensikexperten sowie Strategen. Das Team besteht aus echten Global Playern, bietet innovative Lösungen an und verfügt über Praxiserfahrung in allen grossen EU-Volkswirtschaften.

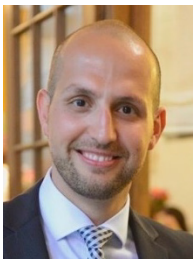
PwC ist bestens aufgestellt, um Sie auf Ihrem Weg zur Konformität – von der Status-quo-Bewertung bis hin zur Umsetzung erforderlicher Massnahmen (siehe Abbildung rechts) – zu unterstützen.

1 Einschätzung der Reaktionsfähigkeit und Gap-Analyse	Wir können Ihnen sagen, wo Sie stehen in Bezug auf die Einhaltung der bestehenden und kommenden Vorschriften
2 Bestand von personenbezogenen Daten	Wir können Ihnen bei der effizienten Sammlung von wichtigen Informationen zu Ihrem Datenbestand und der Definition der Datenverarbeitungsmassnahmen in Ihrer Organisation helfen
3 Erarbeitung eines Aktionsplans	Wir können Ihnen helfen, einen angemessenen Aktionsplan zu erarbeiten und die erforderlichen Prozesse mit Fokus auf Priorisierung und einem risikobasierten Ansatz umzusetzen
4 Umsetzung von Compliance-Massnahmen	Sobald alle Compliance-Gaps und -Massnahmen definiert sind, können wir Ihnen bei der Umsetzung der Prozesse und dem reibungslosen Übergang zu Business as Usual helfen

Anmerkungen

Für weitere Informationen wenden Sie sich bitte an unsere Regulatory Transformation Experten:

Patrick Akiki
Partner
Finance Risk and Regulatory Transformation
Mobile: +41 79 708 11 07
E-Mail: patrick.akiki@ch.pwc.com

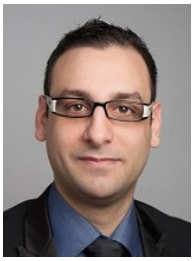


Morris Naqib
Senior Manager,
Risk and Regulatory Transformation
Mobile: +41 79 902 31 45
E-Mail: morris.naqib@ch.pwc.com

Mark Hussey
Senior Manager,
Risk and Regulatory Transformation
Mobile: +41 79 549 07 59
E-Mail: mark.hussey@ch.pwc.com

Isabella Sorace
Manager,
Risk and Regulatory Transformation
Mobile: +41 79 742 37 16
E-Mail: isabella.sorace@ch.pwc.com

Rechtliche Beratung:



Yari Antonio Iannelli
Assistant Manager,
Legal, FS Regulatory & Compliance Services
Mobile: +41 58 792 28 54
Email: yari.iannelli@ch.pwc.com

Wichtige Mitwirkende:
Vielen Dank an Dat Huynh und Enrico Zurkirchen für ihren wertvollen Beitrag zu dieser Publikation.