Regulatorische Entwicklungen

Weitere regulatorische Entwicklungen

Letztes Update: Mai 2024

pwc

Inhaltsverzeichnis

1 Rechtliche Entwicklungen

1.1 Datenschutz-Grundverordnung der EU (GDPR)

Die EU-DSGVO (GDPR) implementiert strikte rechtliche Rahmenbedingungen für den Datenschutz und die Privatsphäre in und ausserhalb von Europa in Bezug auf die Verarbeitung personenbezogener Daten. Die Regelung wurde von den EWR-Staaten übernommen.

Status:
- In Kraft seit 25. Mai 2018

Anwendbarkeit von strikteren EU-Datenschutzbestimmungen

Die Datenschutz-Grundverordnung (EU-DSGVO) gilt seit dem 25. Mai 2018. Diese schuf einen neuen Rechtsrahmen für die Datenschutzgesetze in den 28 Mitgliedstaaten der Europäischen Union (EU) und ersetzte die vorherige EU-Datenschutzrichtlinie.
Die EU-DSGVO implementiert strikte rechtliche Rahmenbedingungen für den Datenschutz und die Privatsphäre in und ausserhalb von Europa in Bezug auf die Verarbeitung von personenbezogenen Daten. Mittels Beschlusses des gemeinsamen EWR-Ausschusses vom 6. Juli 2018 wurde die DSGVO in das EWR-Abkommen übernommen und gilt seit dem 20. Juli 2018 auch in Island, Norwegen und im Fürstentum Liechtenstein.

Compliance-Reise

Die Bestimmungen der EU-DSGVO verlangen von Unternehmen eine Bestandsaufnahme und Anpassung ihrer Systeme sowie der operativen Abläufe in Bezug auf den Datenschutz. In ihrer Gesamtheit legen die Regelungen eine „Compliance-Reise“ fest, der Organisationen folgen müssen, um die Einhaltung der Vorgaben sicherzustellen. Die EU-DSGVO stellt für viele Unternehmen eine grosse, vielschichtige Herausforderung dar, speziell für jene mit umfassenden Archiven, zahlreicher Einbindung von Drittfirmen/Auftragsdatenverarbeitern sowie komplexen IT-Systemlandschaften. Die Umsetzung der Anforderungen beinhaltet zahlreiche Herausforderungen und gestaltet sich oft sehr vielschichtig. Die regulatorischen und operationellen Risiken sind erheblich, vor allem für Unternehmen mit einer auf der kommerziellen Nutzung von personenbezogenen Daten beruhenden Geschäftstätigkeit. Schwere Verstösse sind bereits mit Geldbussen von über EUR 200 Mio. geahndet worden, Millionenbeträge stellen für grössere Unternehmen keine Seltenheit dar. So können Verstösse gegen die Verordnung denn auch mit einer Busse von bis zu EUR 20 Mio. oder 4 % des Jahresumsatzes (evtl. weltweit) bestraft werden – je nachdem, welcher Betrag höher ist. Die EU-DSGVO regelt auch den internationalen Datentransfer. Für grenzüberschreitende Datentransfers gelten strenge Voraussetzungen, die analysiert werden müssen. Organisationen tragen die Verantwortung, grenzüberschreitende Datentransfers angemessen zu sichern. Dies gilt für bereits bestehende sowie für neue Transfers von personenbezogenen Daten, insbesondere in sogenannte „Drittländer“ (Länder ausserhalb der EU und des EWR).

Die Datenschutzgrundsätze der EU-DSGVO müssen stets eingehalten werden. Prinzipien wie Speicherbegrenzung, Datenminimierung oder Rechtmässigkeit gehören zum datenschutzrechtlichen Standard bei der Verarbeitung von personenbezogenen Daten. Es besteht zudem eine sogenannte „Rechenschaftspflicht“, welche Firmen dazu verpflichtet, die Einhaltung der EU-DSGVO nachweisen zu können. Dies gilt einerseits gegenüber den Datenschutzbehörden, ist andererseits aber auch für interne oder externe Stakeholder höchst relevant. Ebenso muss den Rechten der betroffenen Personen fristgerecht entsprochen werden. Insbesondere das Recht auf Löschung („Recht auf Vergessenwerden“) stellt Unternehmen sowie die zum Teil sehr komplexe IT-Landschaft innerhalb einer Organisation vor erhebliche Herausforderungen.

Da die EU-DSGVO eine wichtige Neuerung im Datenschutzrecht darstellt, ist auch nach Ablauf der zweijährigen Übergangsfrist und der Implementierung im Unternehmen die weitere Entwicklung sorgfältig zu analysieren. Die Aktivitäten der Aufsichtsbehörden und die datenschutzrechtliche Rechtsprechung bedingen ein laufendes und institutionalisiertes Monitoring durch das Unternehmen.

Wer ist betroffen?

Die EU-DSGVO geht in ihrem Umfang weiter als die vorhergehende EU-Datenschutzrichtlinie. Jede in Europa aktive Organisation, die personenbezogene Daten verarbeitet, hat die Bestimmungen der EU-DSGVO einzuhalten. Dies gilt auch für jene, die zwar keine Niederlassungen in der EU haben, jedoch Waren und Dienstleistungen an Personen in der EU anbieten oder das Verhalten von Personen beobachten, die sich in der EU befinden. So hat beispielsweise ein Schweizer Händler ohne Niederlassungen in der EU, aber mit an Käufern in der EU gerichteten Marketingaktivitäten die Vorschriften der EU-DSGVO einzuhalten. Dasselbe gilt für Unternehmen, die ihre Produkte oder Dienstleistungen im EWR anbieten oder dort das Verhalten von Personen beobachten.

Was ist zu tun?

Nachdem die EU-DSGVO bereits in Kraft getreten ist, ist davon auszugehen, dass schon ein Grossteil der neuen Vorgaben bei Ihnen im Unternehmen umgesetzt worden ist.

Wir empfehlen daher folgende weitere Schritte:
- Identifizierung der Lücken zwischen Ihrem aktuellen Datenschutzprogramm und den Vorgaben der EU-DSGVO, auch unter Berücksichtigung Ihrer Auftragsdatenverarbeiter
- Anpassung und Verbesserung der operationellen Strukturen, um die Einhaltung der Vorgaben sicherzustellen; dies beinhaltet eine umfangreiche Dokumentation Ihrer Datenschutzprozesse sowie der entsprechenden Kontrollen
- Datenschutzprüfungen und -zertifizierungen sind zu erwägen, um die Datenschutz-Compliance intern und extern nachweisen zu können

Gerne unterstützt Sie Ihr PwC-Datenschutzexperte bei der Erhöhung Ihres Datenschutzniveaus und der Sicherstellung Ihrer Rechenschaftspflicht.

1.2 Revidiertes Bundesgesetz über den Datenschutz (nDSG)

Das schweizerische Datenschutzrecht wird revidiert, besonders das nDSG und die Verordnung zum DSG (VDSG). Das nDSG wird der Datenschutz-Grundverordnung der EU nachgebildet, allerdings mit teils gewichtigen Abweichungen.

Status:
- Inkraftsetzung am 1. September 2023

Revision des Datenschutzgesetzes

Am 15. September 2017 veröffentlichte der Bundesrat den Gesetzesentwurf für die Revision des Bundesgesetzes über den Datenschutz. Sinn und Zweck dieser Gesetzesrevision war es, den Schutz von Personendaten zu stärken und die bestehenden Bestimmungen an das digitale Zeitalter anzupassen. Weiter bezweckte die Revision eine Anpassung des Schweizer Datenschutzgesetzes an die europäische Gesetzgebung, d. h. an die Datenschutz-Grundverordnung der EU (EU-DSGVO). Fast genau drei Jahre nach der Veröffentlichung des ersten Entwurfs wurde die Vorlage nach diversen Differenzen und einer Einigungskonferenz zwischen National- und Ständerat von beiden Räten am 25. September 2020 angenommen.

Ein Faktor, der die Revision des DSG während den drei Jahren der Beratung geprägt hat, war die Sicherstellung des uneingeschränkten Zugangs zum EU-Binnenmarkt. Aufgrund des von der EU-Kommission ausgeübten Drucks in dieser Sache scheinen heute gewisse Teile

der Datenschutzgesetzgebung der EU bewusst in Schweizer Recht übernommen worden zu sein. Dies tat man, um sicherstellen zu können, dass die Schweiz von der EU weiterhin als Drittstaat mit angemessenem Datenschutz angesehen wird und somit von grenzüberschreitendem Datentransfer ohne zusätzliche rechtliche Schutzmassnahmen profitieren kann.

Kernelemente der Gesetzesvorlage und Unterschiede zur EU-DSGVO

Wie die EU-DSGVO zielt die schweizerische Gesetzesvorlage grundsätzlich darauf ab, die Transparenz bei der Datenbearbeitung zu erhöhen und die Strafverfolgung bei Datenschutzverletzungen zu verschärfen. Tatsächlich wird in verschiedenen Bereichen die entsprechende Rechtsterminologie der EU übernommen.

Des Weiteren wird ein risikobasierter Ansatz verfolgt; so nehmen z. B. die Datenschutzpflichten des Datenverantwortlichen im Verhältnis zu den Risiken für die Privatsphäre der betroffenen Personen zu. Wie die EU-DSGVO verpflichtet das revidierte Gesetz grundsätzlich alle Datenverantwortlichen und -bearbeiter, ihre Aktivitäten im Zusammenhang mit der Bearbeitung von Daten zu dokumentieren (Verzeichnis der Bearbeitungstätigkeiten). Hinzukommend stärkt das revidierte DSG (nDSG) entsprechend der Entwicklung in der EU die Rolle und Position des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).

In einigen Bereichen unterscheidet sich der Gesetzestext jedoch grundlegend vom EU-Recht. So sieht er nicht vor, dass Datenverantwortliche im Sinne einer Rechenschaftspflicht die Einhaltung des nDSG dokumentieren müssen. Im Gegensatz zur EU-DSGVO kommt es dadurch beim Datenschutz nicht zu einer Umkehr der Beweislast. Auch enthält der Gesetzesentwurf keine spezifischen Bestimmungen im Hinblick auf den Kindesschutz.

Weitere Unterschiede zur EU-DSGVO ergeben sich bei der Strafverfolgung. Der Höchstwert für Bussen liegt bei CHF 250’000 und ist damit erheblich tiefer als in der EU. Ausserdem werden nach nDSG weiterhin die verantwortlichen Mitarbeitenden (natürliche Personen) strafrechtlich belangt und nicht wie bei der EU-DSGVO die verantwortlichen Stellen (Unternehmen).

Folgen der Revision und Ablauf der Inkraftsetzung

Aufgrund der Tatsache, dass die Verabschiedung des nDSG einen grossen Schritt in Richtung der von der EU-Kommission gewünschten Datenschutzanpassung der Schweiz darstellt, ist die Gefahr, dass die EU diese als unzureichend erachtet nun vorderhand wohl relativ klein. Die Schweiz dürfte damit von der EU im datenschutzrechtlichen Bereich weiterhin als gleichwertig anerkannt werden. Dies ist besonders wichtig für die Schweizer Wirtschaft.

Was ist zu tun?

Wir empfehlen, dass sich Unternehmen mit den Neuerungen im nDSG befassen. Dies speziell, wenn durch das Unternehmen bisher keine Massnahmen hinsichtlich der EU-DSGVO ergriffen wurden.

In der Schweiz tätige Unternehmen müssen sich im Rahmen dessen ein vollständiges Bild davon machen, wie sie Personendaten bearbeiten. Im Anschluss an diese Analyse und durch das Befolgen eines risikoorientierten Ansatzes sollten die notwendigen Massnahmen getroffen werden, um in Zukunft sicherzustellen, dass bei der Datenbearbeitung die neue Gesetzgebung eingehalten wird. Gerne unterstützt Sie Ihr PwC-Datenschutzexperte bei der Anpassung an die neuen Rahmenbedingungen.

2 International Standards on Auditing (ISA)

2.1 ISA 600 (Revised) „Besondere Überlegungen zu Konzernabschlussprüfungen (einschliesslich der Tätigkeit von Teilbereichsprüfern)“

Der Standard stärkt und erweitert die Verantwortung des Group Engagement Leaders für das Management und das Erreichen der Prüfungsqualität im Rahmen der Prüfung eines Konzernabschlusses sowie die Verantwortung des Konzernprüfers für die Gesamtleitung und Überwachung der Konzernabschlussprüfung und die Überprüfung der Arbeit der Teilbereichsprüfer.

Status:	• Anzuwenden ist der Standard für Abschlussprüfungen von Geschäftsjahren, die am oder nach dem 15. Dezember 2023 beginnen

Zu den wesentlichen Änderungen am Standard gehören:

- Die Verantwortung des Konzernprüfers für die Konzernabschlussprüfung zusammen mit einer Änderung der Definition des Prüfungsteams.
- Der Konzernprüfer bestimmt die Teilbereiche, in denen die Prüfungsarbeiten durchgeführt werden (zu diesem Zweck wurde das Konzept der „wesentlichen Teilbereiche“ und die „Prüferische Durchsicht der Finanzinformationen der Teilbereiche“ als Tätigkeitstyp abgeschafft), sowie Art, Zeitpunkt und Umfang, in dem die Teilbereichsprüfer beteiligt werden sollen.