November 2020

Newsletter Nr. 146

Das revidierte Datenschutzgesetz – Empfehlungen zur Umsetzung

Das revidierte Datenschutzgesetz tritt voraussichtlich anfangs bis Mitte 2022 in Kraft. Es enthält kaum praktisch relevante Übergangsfristen – Pflichten wie bspw. die Informationspflicht, die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung oder zur Meldung von Datensicherheitsverletzungen gelten weitgehend ab dem Inkrafttreten. Die rechtzeitige Einhaltung dieser Pflichten verlangt Vorbereitung. Ziele und Umfang von Umsetzungsprojekten schwanken dabei stark, abhängig z.B. von Grösse und Komplexität des Unternehmens, dem Geschäftsmodell, den Erwartungen an die betreffende Branche und ob Vorgaben der Datenschutzgrundverordnung (DSGVO) bereits implementiert wurden. Ein pragmatisches und zielorientiertes Vorgehen ist dabei essenziell.

walderwyss rechtsanwälte

Von Jürg Schneider
Dr. iur., Rechtsanwalt
Partner
Telefon direkt: +41 58 658 55 71
juerg.schneider@walderwyss.com

und David Vasella
Dr. iur., Rechtsanwalt
Partner
Telefon direkt: +41 58 658 52 87
david.vasella@walderwyss.com

und Lena Götzinger
Rechtsanwältin (Rechtsanwaltskammer Frankfurt am Main)
Associate
Telefon direkt: +41 58 658 56 63
lena.goetzinger@walderwyss.com

Das geltende schweizerische Datenschutzgesetz (**DSG**) ist seit 1993 in Kraft. Seither hat die Digitalisierung Geschäftsmodelle, die Risiken für Betroffene und die Erwartungen an den Datenschutz stark verändert. Im EWR gilt seit Mai 2018 die DSGVO, und die Europaratskonvention 108 wurde revidiert. Auch das DSG wird revidiert, in vielen Punkten entlang der DSGVO. Das führt zu Verschärfungen sowohl der Pflichten als auch der Risiken für Unternehmen, und die Stellung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (**EDÖB**) wurde deutlich gestärkt.

Anders als die DSGVO betrifft das revidierte DSG alle Unternehmen, die einen Sitz in der Schweiz haben oder deren Bearbeitungen sich hier auswirken – auch Unternehmen ohne Berührung mit ausländischen Märkten. Sonderbestimmungen für KMU finden sich kaum. Vorbereitungs- bzw. Umsetzungsmassnahmen sind deshalb notwendig, nicht nur bei Unternehmen, die in regulierten Branchen tätig sind, die besonders heikle oder umfangreiche Daten bearbeiten oder die im Fokus der Öffentlichkeit stehen.

Erfolgreich und nachhaltig ist eine Umsetzung aber nur, wenn sie der Komplexität des Umfelds und den Risiken und den Rahmenbedingungen des Unternehmens Rechnung trägt. Ein One-Size-Fits-All-Ansatz ist ebenso verfehlt wie eine detailbesessene Umsetzung. Ein pragmatischer und zielorientierter Ansatz ist essenziell.

Die wichtigsten Neuerungen

Das revidierte Datenschutzgesetz (**revDSG**) wurde am 25. September 2020 vom Parlament verabschiedet. Diese Revision macht auch eine Überarbeitung des Verordnungsrechts erforderlich, besonders der Verordnung zum DSG (**VDSG**). Mit dem Beginn einer Vernehmlassung zur revidierten VDSG (**revVDSG**) ist derzeit auf Mitte 2021 zu rechnen. RevVDSG und revDSG werden voraussichtlich beide anfangs bis Mitte 2022 in Kraft treten.

Einige Neuerungen werden sich in der Praxis auswirken, haben für die Compliance im Unternehmen aber eine geringere Bedeutung, z.B. die Beschränkung des revDSG auf Daten natürlicher Personen. Die folgenden Punkte stehen bei der Umsetzung dagegen im Vordergrund:

i. Verantwortliche und Auftragsbearbeiter haben ein Inventar ihrer Bearbeitungstätigkeiten zu führen ("Bearbeitungsverzeichnis"), analog zur entsprechenden Pflicht nach der DSGVO.

ii. Verantwortliche können einen Datenschutzberater bestellen, was Erleichterungen im Zusammenhang mit Datenschutz-Folgenabschätzungen (**DSFA**) bewirkt.

iii. Das revDSG sieht eine Informationspflicht grundsätzlich bei jeder Beschaffung von Daten vor, die nicht mehr nur bei besonders schützenswerten Daten gilt. Dagegen werden keine neuen Einwilligungserfordernisse geschaffen, auch nicht z.B. für ein Profiling.

iv. Das Datenschutzrecht verlangt einen angemessenen Umgang mit Risiken für Betroffene. Dazu gehört, dass der Verantwortliche bereits bei der Planung von Bearbeitungen Risiken berücksichtigt und bewusst entscheidet, wie er den Datenschutz angemessen einhalten kann ("Privacy by Design"). Bei heikleren Bearbeitungen muss die Risikoeinschätzung in Form einer DSFA erfolgen und dokumentiert werden.

v. Verantwortliche mit Sitz im Ausland haben unter bestimmten Voraussetzungen einen Vertreter in der Schweiz zu bestellen.

vi. Bei der Zusammenarbeit mit Kunden, Lieferanten und Partnern sind die datenschutzrechtlichen Rechte und Pflichten vertraglich zu regeln, z.B. durch Vereinbarungen zwischen Verantwortlichen und Auftragsbearbeitern.

vii. Die Rechte der Betroffenen werden gestärkt. Neu ist das Recht auf eine Kopie bestimmter Daten in maschinenlesbarer Form.

viii. Weiterhin wichtig bleibt die rechtzeitige Löschung oder Anonymisierung von Personendaten.

ix. Bei bestimmten vorsätzlichen Verstössen können die handelnden Personen mit Bussen bis zu CHF 250'000 bestraft werden. Unternehmen können unter bestimmten Voraussetzungen anstelle dieser Personen mit einer Busse bis zu CHF 50'000 bestraft werden. Zudem bestehen Haftungsrisiken, operationelle Risiken durch ein mögliches Einschreiten des EDÖB und vor allem Reputationsrisiken.

Umsetzung

Die Umsetzung des revDSG erfordert frühzeitige Planung. Die zentralen Schritte sind aber häufig mit relativ niedrigem Aufwand möglich. Möglich und sinnvoll ist oft auch ein stufenweises Vorgehen, bei dem bestimmte Massnahmen prioritär und weitere Massnahmen in einer zweiten Phase in Angriff genommen werden. Der Umfang der Umsetzung hängt schliesslich auch davon ab, ob die DSGVO bereits umgesetzt worden ist oder nicht.

Klärung des Umsetzungsbedarfs. Noch vor dem Beginn eines Umsetzungsprojekts sollte das Unternehmen – bzw. die Unternehmensgruppe – den relevanten Rechtsrahmen bestimmen. Finden die DSGVO und nationales Recht von EWR-Mitgliedstaaten Anwendung? Finden zusätzlich sektorielle Bestimmungen in der Schweiz oder auch im Ausland Anwendung, z.B. Geheimnisschutzbestimmungen oder Bestimmungen des Versicherungs-, Finanzmarkt-, Gesundheits- oder Humanforschungsrechts? Handelt das Unternehmen als Privater oder (auch) als Bundesorgan? In diesem Zusammenhang kann auch entschieden werden, ob und inwieweit eine freiwillige Anwendung der DSGVO sinnvoll ist.

Bearbeitungsverzeichnis. Sowohl die DSGVO als auch das revDSG verlangen die Aufnahme von "Bearbeitungsverzeichnissen", d.h. von Inventaren, in denen die unterschiedlichen Bearbeitungstätigkeiten erfasst werden (sowohl durch Verantwortliche als auch Auftragsbearbeiter). Bei KMU können Ausnahmen greifen. Die Aufnahme der Verzeichnisse zumindest in bestimmten Bereichen – oft unterstützt durch entsprechende technische Lösungen – ist meist ein sinnvoller erster Schritt, weil sie eine gewisse Klarheit schafft und dazu beiträgt, das Unternehmen bzw. die zuständigen Personen und Funktionen auf weitere Umsetzungsmassnahmen vorzubereiten. Haben Unternehmen bereits im Rahmen der DSGVO Bearbeitungsverzeichnisse angelegt, dürften diese auch die Anforderungen nach den revDSG abdecken. Ebenso wichtig wie die Erstellung der Bearbeitungsverzeichnisse ist sodann ihre Pflege. Zu planen sind daher Prozesse, wie neue oder geänderte Bearbeitungen erfasst werden.

Interne Verantwortlichkeiten. Unternehmen brauchen eine angemessene Struktur und die notwendigen Kompetenzen für die Einhaltung datenschutzrechtlicher Pflichten, falls eine solche nicht bereits besteht. Bei Anwendbarkeit der DSGVO ist ggf. ein Datenschutzbeauftragter zu bestellen, wenn die Voraussetzungen der DSGVO oder nationaler Rechte erfüllt sind. Eine solche Pflicht besteht unter dem revDSG nicht, doch kann die freiwillige Bestellung eines Datenschutzberaters Vorteile bieten, wie besonders die Befreiung von der Meldepflicht an den EDÖB (vgl. Art. 23 Abs. 4 revDSG).

Weitere Dokumentation. Anders als die DSGVO kennt das revDSG keine allgemeine Pflicht des Verantwortlichen, die Einhaltung des Datenschutzrechts umfassend zu dokumentieren. Eine Dokumentation in gewissem Umfang ist dennoch notwendig. Mit Blick auf die allgemeinen Bearbeitungsprinzipien und besondere sektorielle Bestimmungen ist ausserdem zu empfehlen, die Mitarbeiter in den entsprechenden Abteilungen zu schulen. Sinnvoll oder sogar notwendig ist weiter, Richtlinien, Leitfäden und Merkblätter zu erarbeiten. Bestehen solche bereits nach der DSGVO, sind diese – mit beschränktem Aufwand – an das revDSG anzupassen.

Transparenz, Einwilligungen und Information. Das revDSG führt eine neue, allgemeine und aktive Informationspflicht ein, ergänzend zum Transparenzgrundsatz, deren Verletzung strafbedroht ist. Zu prüfen ist daher zunächst, wo und wie Personendaten beschafft werden und welche Datenschutzhinweise bereits in Verwendung sind (z.B. in Datenschutzerklärungen oder AGB). Das revDSG stellt hier in wenigen Punkte strengere Anforderungen als die DSGVO. Zu klären ist weiter, ob und wo Einwilligungen der Betroffenen erforderlich oder sinnvoll sind und in welcher Form diese eingeholt werden können. Ein Einwilligungserfordernis kann sich auch aus anderen Gesetzen ergeben, z.B. bei Geheimhaltungspflichten.

Zusammenarbeit mit Dritten. In der Zusammenarbeit mit Lieferanten und Kunden, aber auch bei konzerninternen Datenflüssen sind die datenschutzrechtlichen Zuständigkeiten und Verantwortlichkeiten zu bestimmen und zu

vereinbaren. Zwischen Auftragsbearbeiter und Verantwortlichem ist auch nach dem revDSG eine Vereinbarung zu treffen, die schriftlich erfolgen sollte. Inhaltlich gehen die Anforderungen allerdings weniger weit als nach der DSGVO, deren Anforderungen sich zum Standard entwickelt haben. Auch bei gemeinsamer Verantwortung und dem Datenaustausch zwischen unabhängigen Verantwortlichen können entsprechende Vereinbarungen notwendig sein.

Datensicherheit und Sicherheitsverletzungen. Unternehmen müssen sicherstellen, dass Datenbearbeitungen am Prinzip der datenschutzfreundlichen Voreinstellungen ausgerichtet werden, dass die Datensicherheit weiterhin gewährleistet ist und dass Verletzungen der Datensicherheit erkannt, intern kommuniziert, ggf. eskaliert und unter Umständen auch dem EDÖB bzw. den zuständigen Behörden oder den betroffenen Personen mitgeteilt werden. Diese Pflicht gilt parallel zu etwaigen spezialgesetzlichen Meldepflichten etwa von Finanzinstituten.

Betroffenenrechte. Die bereits heute bestehenden Betroffenenrechte werden teilweise anders gefasst und durch das neue Recht auf Datenportabilität ergänzt. Dafür sind Prozesse zu entwickeln, falls Betroffenenanfragen häufig sind. Auch Unternehmen, welche die DSGVO bereits umgesetzt haben, sollten dies prüfen, weil das revDSG in einigen – aber wichtigen – Punkten von der DSGVO abweicht.

Datenschutzrechtliche Compliance verlangt Planung

Die Umsetzung der DSGVO und des revDSG ist nicht unbedingt aufwendig, verlangt aber Planung. Schon aus Gründen der Budgetierung und des Reportings ist eine konkrete Planung notwendig, auch damit auf Änderungen und Verzögerungen richtig reagiert werden kann. Walder Wyss AG kann mit einer praxiserprobten Toolbox aus Anleitungen, Checklisten und Vorlagen unterstützen, die Aufwand, Zeitbedarf und Kosten reduzieren. Unternehmen stellen wir gerne auch einen Leitfaden zur Umsetzung zur Verfügung – wenden Sie sich gerne an uns.