Die Auswirkungen des neuen Datenschutzgesetzes auf KMU

Von RA lic. jur. Ursula Sury

Am 25. September 2020 wurde das neue Datenschutzgesetz durch das Parlament verabschiedet. Es unterliegt momentan der Referendumsfrist und nach Ablauf dieser wird über das Inkrafttreten entschieden. Es wird mit dem Inkrafttreten im Jahr 2022 gerechnet. Das neue Datenschutzgesetz orientiert sich an der DSGVO der EU und enthält Änderungen, die für Unternehmen von Bedeutung sind. Dieser Artikel behandelt die wichtigsten Änderungen sowie die Massnahmen, die KMU treffen sollten.

Grundsätze der Datenbearbeitung

Die Grundsätze der Datenbearbeitung bleiben weitgehend dieselben. Datenbearbeitungen sind in der Regel zulässig, auch ohne Einwilligung, und nur in bestimmten Fällen ist ein Rechtfertigungsgrund nötig. Dies bleibt ein Unterschied zur DSGVO, gemäss dieser sind Datenbearbeitungen grundsätzlich verboten, ausser es gibt einen Rechtfertigungsgrund. Neu ist, dass sich der Anwendungsbereich des Datenschutzgesetzes beschränkt auf die Bearbeitung von Personendaten natürlicher Personen und juristische Personen nicht mehr geschützt sind (Art. 2 nDSG).

Neuerungen

«Privacy by Design» und «Privacy by Default»

Die Prinzipien «Privacy by Desgin» sowie «Privacy by Default» sind im neuen Datenschutzgesetz geregelt (Art. 7 nDSG). «Privacy by Design» beinhaltet, dass das Thema Datenschutz schon bei der Entwicklung von Technologien berücksichtigt wird und nicht erst im Nachhinein. So werden Risiken durch Softwarelösungen vorgebeugt und es kann gleichzeitig darauf geachtet werden, dass deren Funktionalität gewährleistet wird. «Privacy by Default» setzt voraus, dass die Bearbeitung von Personendaten auf das für den Verwendungszweck nötige Mindestmass reduziert ist. Dies ist mittels geeigneter Voreinstellungen sicherzustellen.

Auftragsbearbeiter

Die Reglungen zum Beizug eines Auftragsbearbeiters bleiben die gleichen. Neu ist aber gesetzlich festgehalten, dass der Auftragsbearbeiter nur mit Zustimmung des für die Daten Verantwortlichen Unternehmens einen Dritten beiziehen darf (Art. 9 nDSG). Dies ist auch in der DSGVO so geregelt.

Informationspflicht

Die Informationspflicht bei Datenbeschaffungen wird ausgeweitet (Art. 19 ff. nDSG). Eine Datenschutzerklärung muss erstellt werden, da die betroffenen Personen nicht mehr nur über die Datenbeschaffung bei besonders schützenswerten Personendaten informiert werden müssen, sondern eine Informationspflicht bei jeder Datenbeschaffung besteht. Die Mindestangaben sind gesetzlich geregelt. Das Unternehmen, das die Daten beschafft muss der betroffenen Person mindestens die Identität und die Kontaktdaten des Verantwortlichen, den Bearbeitungszweck sowie gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden mitteilen. Diese Mindestangaben sind weniger umfassend, als jene nach der DSGVO.

Das neue Datenschutzgesetz geht bei der Informationspflicht bei Datenbekanntgaben ins Ausland weiter als die DSGVO. Wenn Personendaten ins Ausland bekanntgegeben werden, müssen der betroffenen Person der entsprechende Staat oder das internationale Organ bekanntgegeben werden.

Neu ist zudem die Informationspflicht bei einer automatisierten Einzelentscheidung (Art. 21 nDSG). Eine automatisierte Einzelentscheidung liegt vor, wenn eine Entscheidung ausschliesslich auf einer automatisierten Bearbeitung beruht. Die Informationspflicht über eine solche Entscheidung besteht, wenn für die betroffene Person eine Rechtsfolge damit verbunden ist oder sie erheblich beeinträchtigt wird.

Wer vorsätzlich gegen diese Informationspflichten verstösst, kann mit einer Busse bis zu CHF 250'000.- bestraft werden (Art. 60 nDSG).

Datenschutz-Folgeabschätzung

Datenverantwortliche oder Datenverarbeiter müssen nach dem neuen Datenschutzgesetz eine Datenschutz-Folgenabschätzung vornehmen, wenn die vorgesehene Datenverarbeitung zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führt (Art. 22 nDSG). In der Datenschutz-Folgeabschätzung muss die geplante Bearbeitung beschrieben werden, die Risiken für die Grundrechte und die Persönlichkeit der betroffenen Person bewertet sowie die Massnahmen zum Schutz dieser benannt werden.

Meldung von Verletzungen der Datensicherheit

Ist die Datensicherheit verletzt und kann dies zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen, muss dies dem EDÖB gemeldet werden (Art. 24 nDSG). Die Meldung muss mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die vorgesehenen oder bereits ergriffenen Massnahmen enthalten.

Datenschutzberater

Unternehmen können einen Datenschutzberater ernennen (Art. 10 nDSG). Sie sind aber nicht dazu verpflichtet. Vorteil der Ernennung eines Datenschutzberaters ist, dass klar festgelegt wird, wer Anlaufstelle für Personen, über die Daten bearbeitet werden sowie Behörden ist. Die Aufgaben des Datenschutzberaters sind die Schulung und Beratung des Unternehmens in Datenschutzfragen sowie die Mitwirkung bei der Anwendung der Datenschutzvorschriften.

Ein weiterer Vorteil ist, dass ein Unternehmen, das eine Datenschutz-Folgeabschätzung erstellt und diese meldepflichtig ist, den EDÖB nicht konsultieren muss, da es den eigenen Datenschutzberater konsultieren kann. Eine meldepflichtige Datenschutz-Folgeabschätzung liegt vor, wenn die Bearbeitung trotz der vorgesehenen Massnahmen immer noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hat.

Massnahmen

Nachfolgend werden die grundlegengen potenziellen Massnahmen für KMU zusammengefasst aufgeführt:

- Bei der Entwicklung neuer Technologien den Datenschutz einbeziehen und die Bearbeitung von Personendaten auf ein Mindestmass reduzieren.
- Datenschutzerklärung erstellen oder schon bestehende prüfen und anpassen.
- Auslandtransfer identifizieren und Informationspflicht erfüllen.

- Prozess für die Datenschutz-Folgeabschätzung bei Datenbearbeitungen mit hohem Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen erarbeiten und umsetzen.
- Es wird empfohlen, einen Datenschutzberater zu ernennen, wenn meldepflichtige Datenschutz-Folgeabschätzungen im Unternehmen vorliegen.
- Prozess für die Meldungen von Verletzungen der Datensicherheit festlegen.
- Die Verträge mit Auftragsbearbeitern auf DSG-Konformität überprüfen und gegebenenfalls anpassen.
- Alle getroffenen Massnahmen aus Sorgfaltspflichtgründen dokumentieren, da sonst hohe Bussen drohen können.

Grundsätzlich kann festgehalten werden, dass für Unternehmen, die bereits DSGVO-konform arbeiten, wenig Handlungsbedarf entsteht, da sie viele Voraussetzungen des neuen Datenschutzgesetzes bereits erfüllen.

Fazit

Das neue Datenschutzgesetz tritt voraussichtlich 2022 in Kraft. Es ist eine Annäherung an die DSGVO und bringt einige Änderungen mit sich. So werden insbesondere die Informationspflichten ausgeweitet, bei einer Datenbearbeitung mit hohem Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person muss eine Datenschutz-Folgeabschätzung erstellt werden und es besteht eine gesetzliche Pflicht zur Meldung von Verletzung der Datensicherheit an den EDÖB. Die Neuerungen müssen durch KMU umgesetzt werden. Es ist unter anderem wichtig, eine Datenschutzerklärung zu erstellen oder eine schon bestehende zu prüfen. Aufgrund der Sorgfaltspflicht wird dringend empfohlen, sämtliche Massnahmen zu dokumentieren, um im Zweifelsfall Bussen zu vermeiden.

Ursula Sury ist selbständige Rechtsanwältin in Luzern (CH) und Vizedirektorin an der Hochschule Luzern – Informatik. Sie ist zudem Dozentin für Informatikrecht in verschiedenen Nachdiplomstudien, welche am Institut für Wirtschaftsinformatik der Hochschule durchgeführt werden. Die Autorin ist hauptsächlich im Bereich Informatikrecht und Datenschutz tätig.