Zeitalter der Digitalisierung: Mindestanforderungen an die Datensicherheit

In diesem Artikel werden die neuen Mindestanforderungen im revidierten Datenschutzgesetz beleuchtet. Mit dem Inkrafttreten sind sowohl Verantwortliche als auch Auftragsbearbeiter mit den Mindestanforderungen konfrontiert. Der Text bietet eine kurze Darstellung der technischen und organisatorischen Massnahmen und erklärt die möglichen Folgen von Verstössen.

Von Florian Müller

1. Rechtliche Grundlagen für Datensicherheit

Am 1. September 2023 tritt das neue Datenschutzgesetz (DSG) und gleichzeitig die neue Datenschutzverordnung (DSV) in Kraft. Damit ändern sich die Mindestanforderungen an die Datensicherheit. Sowohl die Verantwortlichen als auch die Auftragsbearbeiter sind verpflichtet, eine angemessene Datensicherheit zu gewährleisten (Art. 8 Abs. 1 DSG). Diesen gilt es unbedingt Beachtung zu schenken, da ein vorsätzlicher Verstoss gegen die Anforderungen an die Datensicherheit mit Busse von bis zu CHF 250000.– bestraft werden kann. Daneben gilt es auch, nicht leicht wiedergutzumachende Reputationsschäden als Folgeerscheinungen zu beachten, wenn entsprechende Verletzungen publik werden.

Die bundesrechtlichen Mindestanforderungen an die Datensicherheit wurden vom Bundesrat in der DSV unter dem Stichwort «technische und organisatorische Massnahmen» (TOM) festgelegt. Diese Vorschriften gelten für die Verantwortlichen wie auch für Auftragsbearbeiter, welche dem DSG unterstehen. Die Datensicherheit soll präventiv sichergestellt werden, wobei die Sicherstellung nicht absolut erfolgen kann. Mittels geeigneter Sicherheitsarchitektur für die vorhandenen Systeme sollen beispielsweise die Implementierung von Schadsoftware oder der Datenverlust vermieden werden.

Was das im Ergebnis für die TOM bedeutet, soll nachfolgend ausgeführt werden.

2. Technische und organisatorische Massnahmen (TOM)

Art. 8 Abs. 3 DSG ermächtigt den Bundesrat, die Bestimmungen über die Mindestanforderungen an die Datensicherheit zu erlassen. Der Bundesrat hat von dieser Ermächtigung (zu) extensiv Gebrauch gemacht und in der DSV die Mindestanforderungen festgelegt.

Bei den technischen und organisatorischen Massnahmen sind der Stand der Technik und die Implementierungskosten zu berücksichtigen, wobei diese während der gesamten Bearbeitungsdauer zu überprüfen sind (Art. 1 Abs. 4 und 5 DSV). Es sind diejenigen TOM zu treffen, damit die bearbeiteten Daten ihrem Schutzbedarf entsprechend

- nur Berechtigten zugänglich sind (Vertraulichkeit);
- verfügbar sind, wenn sie benötigt werden (Verfügbarkeit);
- nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität);
- nachvollziehbar bearbeitet werden können (Nachvollziehbarkeit).

Ziele der Datensicherheit

Treffen von technischen und organisatorischen Massnahmen zur Sicherstellung der

- Vertraulichkeit,
- Verfügbarkeit,
- Integrität,
- Nachvollziehbarkeit

von Personendaten.

3. Inhalt der Begriffe

Vertraulichkeit im Sinne der Verordnung bedeutet, dass berechtigte Personen nur auf diejenigen Personendaten Zugriff haben, die sie zur Erfüllung ihrer Aufgaben benötigen (Zugriffskontrolle), nur berechtigte Personen Zugang zu den Räumlichkeiten und Anlagen haben, in denen Personendaten bearbeitet werden (Zugangskontrolle) und dass unbefugte Personen automatisierte Datenbearbeitungssysteme nicht mittels Einrichtungen zur Datenübertragung benutzen können (Benutzerkontrolle). Bezüglich Zugriffskontrolle sind insbesondere granular abgestufte Zugriffsberechtigungen umzusetzen. Es soll nicht jeder Mitarbeiter auf alle Daten Zugriff haben, sondern nur auf diejenigen, die zur Erfüllung seiner Aufgaben notwendig sind. Im Sinne der Zugangskontrolle ist sicherzustellen, dass die Räumlichkeiten der Unternehmung und dann insbesondere die Räumlichkeiten mit Personendaten (Büro HR, Serverräume u.Ä.) nicht von Unbefugten betreten werden können. Dies ist möglich durch digitale (Badge-Karten, Fingerabdrücke etc.) oder analoge (Schlüssel) Zugangskontrollen.

Die Anforderungen bezüglich Verfügbarkeit und Integrität sollen grundsätzlich den jederzeitigen Zugriff auf

unveränderte Daten sicherstellen. So sollen unbefugte Kopier-, Veränderungs-, Verschiebungs-, Lösch- oder Vernichtungsvorgänge während eines ganzen Datenzyklus sichergestellt werden. Geschützt werden sollen folglich die Datenträger (Harddisks, Speicherbänder etc.), Speicher (Arbeits- und andere flüchtige Speichermedien) und Transportkanäle (Up- und Downloadkanäle). Für die Verfügbarkeit muss die rasche Wiederherstellung der Systeme und damit der Personendaten sichergestellt sein. Wieder sollen die Systeme stehts auf dem neuesten Sicherheitsstand gehalten und auf korrekte Funktionalität getestet werden. Für die Datenträgerkontrolle können beispielsweise Datenträger mit Passwörtern geschützt werden (z. B. Bitlocker). Für die Wiederherstellung ist wichtig, dass die erstellten Wiederherstellungsdateien auf ihre Nutzbarkeit hin überprüft werden. Nichts ist schlimmer als ein vorhandenes Back-up, welches jedoch nicht mehr gelesen und somit verwendet werden kann. Es sollte folglich in regelmässigen Abständen ein Wiederherstellungstest vorgenommen werden.

Bei der Nachvollziehbarkeit müssen die vorgenommenen Eingaben, Änderungen oder Bekanntgaben überprüft werden können. Weiter sollen Verletzungen der Datensicherheit rasch erkannt und entsprechende Massnahmen zur Minderung oder Beseitigung der Folgen ergriffen werden können.

4. Kontinuierliche Überprüfung

Mithilfe der oben erwähnten Massnahmen sollen Verletzungen der Datensicherheit vermieden werden. Dies bedingt auch, dass die getroffenen Massnahmen regelmässig auf ihre Wirksamkeit hin überprüft werden. Gerade die rasante Entwicklung im Bereich neuer Technologien kann es notwendig machen, dass Sicherheitsmassnahmen ebenfalls dem aktuellen Stand der Technik angepasst werden.

5. Zusammenhängende Pflichten und Sanktionen

Mit Busse bis zu CHF 250 000.– werden private Personen auf Antrag bestraft, die vorsätzlich die Mindestanforderungen an die Datensicherheit, die der Bundesrat erlassen hat, nicht einhalten (Art. 61 lit. c revDSG). Diese Bestimmung wurde neu eingefügt im revidierten DSG. Sie betrifft sowohl den Verantwortlichen als auch den Auftragsbearbeiter.

Der Verantwortliche muss so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt, der Aufsichtsbehörde melden (dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten). In der Meldung nennt er mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen. Je nach Art der Verletzung sind die betroffenen Personen zu informieren.

Die vorliegende Konstellation ist in dem Sinne interessant, als die Nichtmeldung einer Verletzung der Datensicherheit nicht strafbewehrt ist, die Verletzung der Datensicherheit selbst jedoch schon. Es muss jedoch davon ausgegangen werden, dass die Aufsichtsbehörden bei unterlassenen Meldungen eine Untersuchung veranlassen und allfällig administrative Sanktionen aussprechen werden.

6. Kritik an der strafrechtlichen Durchsetzbarkeit

Einer der wichtigsten Grundsätze des Strafrechts ist: Es gibt keine Strafe ohne Gesetz. In der Lehre ist die Kritik erhoben worden, dass die Bestimmungen zur Datensicherheit in der DSV die notwendigen Anforderungen an eine strafrechtliche Norm nicht erfüllen und deswegen auch keine Bussen ausgesprochen werden können.

Die Datenbearbeiter in der Schweiz sind jedoch gut beraten sich nicht auf diese juristisch allenfalls zutreffenden Meinungen zu verlassen und die notwendigen TOMs zu implementieren. Selbst wenn keine strafrechtliche Sanktionierung möglich sein sollte, was wohl erst durch einen langwierigen und finanzintensiven Instanzenzug durch die Gerichte festgestellt werden wird, kann noch immer die Aufsichtsbehörde administrative Massnahmen erlassen. Dies kann von der Verfügung zur Anpassung der Datenbearbeitung bis hin zur Unterlassung reichen, was allenfalls zur notwendigen Einstellung eines Geschäftszweigs führen könnte.

7. Fazit

Im Zeitalter der Digitalisierung muss Schritt gehalten werden mit den technischen Neuerungen, was dazu führt, dass auch die Datensicherheit laufend und regelmässig überprüft werden muss.

Ob nun strafbar oder nicht: Es lohnt sich, die Vorgaben des DSG bzw. der DSV einzuhalten, zumal Bussen verhängt werden können und mögliche Reputationsschäden unbedingt beachtet werden müssen. Ein Unternehmen tut gut daran, die Datensicherheit ernst zu nehmen und sich, falls notwendig, von Experten entsprechend beraten zu lassen.

AUTOR

Florian Müller, berät als Technologie-Anwalt und Notar kleinere und mittlere Unternehmen in den Bereichen IT, Datenschutz, Immaterialgüterrecht (IP), Blockchain sowie weiteren wirtschaftsrechtlichen Bereichen. Er war in einer auf IT-Recht und Datenschutz spezialisierten Kanzlei tätig, bevor er als Senior Associate LEXcellence beitrat.