Jetzt ist die Zeit, um sich vorzubereiten

Datenschutzgesetz | Das totalrevidierte Gesetz tritt voraussichtlich 2022 in Kraft und hat grosse Auswirkungen auf Energieversorgungsunternehmen, aber auch auf alle anderen Betriebe, welche Daten ihrer Kunden bearbeiten. Um den Anforderungen des neuen Datenschutzgesetzes zu entsprechen, müssen Unternehmen technische und organisatorische Massnahmen einleiten und umsetzen.

KLAUS KROHMANN, MARTIN GREUTER

Am 25. September 2020 wurde das totalrevidierte Datenschutzgesetz vom eidgenössischen Parlament verabschiedet. In jener Session stand das Notverordnungsrecht zu Covid-19 im Vordergrund, weshalb die Gesetzesrevision zum Datenschutz etwas in den Hintergrund rückte. Die Revision hat jedoch gewichtige Auswirkungen für Unternehmen und den Einzelnen und hat deshalb durchaus Beachtung verdient: Mit dem Ziel, eine gleichwertige Datenschutzgesetzgebung zur Datenschutz-Grundverordnung der EU (DSGVO) zu schaffen, wurden die Rechte der Betroffenen gestärkt und unter Androhung von verschärften Sanktionen neue Pflichten für Unternehmen geschaffen. Das revidierte Datenschutzgesetz wird voraussichtlich im Jahr 2022 in Kraft treten. Im Unterschied zu den ersten Entwürfen sind keine Übergangsfristen mehr vorgesehen.

Bewährtes Massnahmen-Konzept

Bereits das gegenwärtige Datenschutzgesetz besagt in Artikel 7: «Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.» Der Bundesrat wurde ermächtigt, nähere Bestimmungen zu den technischen und organisatorischen Massnahmen zu erlassen. Der entsprechenden bundesrätlichen

Bild: Tania Rose/pixabay

Verordnung lässt sich entnehmen, dass die Massnahmen folgenden Kriterien Rechnung zu tragen haben: Zweck der Datenbearbeitung, Art und Umfang der Datenbearbeitung sowie Einschätzung der möglichen Risiken für die betroffenen Personen.

Welche konkreten Massnahmen zu treffen sind, wird den Verantwortlichen überlassen, wobei sie einen nicht unerheblichen Entscheidungsspielraum haben: Eine Datenbank mit Gesundheitsdaten und Zehntausenden Betroffenen ist durch strengere Massnahmen zu schützen als die Mitgliederliste des lokalen Fussballvereins mit 150 Einträgen.

Die Verordnung zählt Beispiele für technische und organisatorische Massnahmen auf. Die Beispiele sind jedoch sehr allgemein gehalten. Daher haben verschiedene Behörden und Branchenorganisationen Leitlinien und Empfehlungen herausgegeben, so auch der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte. Oftmals erscheinen diese Leitlinien und Empfehlungen dem Laien sehr theoretisch, und es kann wenig Konkretes abgeleitet werden. Dies ist sicherlich ein Grund, weshalb die technischen und organisatorischen Massnahmen bisher eher auf der theoretischen Ebene blieben.

Typischerweise werden folgende technische und organisatorische Massnahmen unterschieden:

1. Massnahmen zur Pseudonymisierung und Verschlüsselung personenbezogener Daten
- Massnahmen zur Pseudonymisierung personenbezogener Daten
- Massnahmen zur Verschlüsselung personenbezogener Daten

2. Massnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit
- Massnahmen zur Zutrittskontrolle (Physical access control)
- Massnahmen zur Zugangskontrolle (Electronic access control)
- Massnahmen zur Zugriffskontrolle (Logic access control)
- Massnahmen zur Trennungskontrolle (Separation control)

3. Integrität und Unveränderbarkeit
- Massnahmen zur Weitergabekontrolle (Transfer control)
- Massnahmen zur Eingabekontrolle (Input control)

4. Massnahmen, um die Verfügbarkeit der personenbezogenen Daten sicherzustellen
- Massnahmen zur Verfügbarkeitskontrolle (Availability control)

5. Massnahmen, die ein Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen gewährleisten
(Effectivness control)

6. Weisungsrecht und Auftragsüberwachung
- Massnahmen zum Weisungsrecht und zur Auftragserteilung
- Massnahmen zur Auftragskontrolle

Die Bedeutung in Bezug auf das revidierte Datenschutzgesetz

Das revidierte Datenschutzgesetz verpflichtet die Verantwortlichen dazu, technische und organisatorische Massnahmen zu treffen, welche dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem Risiko für den Betroffenen entsprechen. Der Bundesrat ist wiederum ermächtigt, Details dazu auf dem Verordnungsweg zu regeln. Über den Inhalt dieser Verordnung ist jedoch noch nichts bekannt.

Indessen ergeben sich bereits aus dem Gesetz erwähnenswerte Neuerungen:

- Wer die minimalen, vom Bundesrat auf dem Verordnungsweg noch zu bestimmenden, technischen und organisatorischen Massnahmen nicht implementiert, kann auf Antrag mit bis zu 250 000 CHF gebüsst werden. Der Strafdrohung unterstehen in erster Linie die mit der Leitung der jeweiligen Organisation betrauten Personen; bei der Aktiengesellschaft also insbesondere die Mitglieder des Verwaltungsrats, allenfalls auch Geschäftsleitungsmitglieder.
- Alle Organisationen müssen einen Überblick über ihre Datenverarbeitung haben. Dazu werden alle Organisationen eine Art Inventar oder Register über die Prozesse, mit denen Personendaten verarbeitet werden, erstellen müssen. Ab 250 Mitarbeiterinnen und Mitarbeitern sind in diesem Register zwingend Themen zu erheben. Sodann sind bei jedem Prozess das datenschutzrechtliche Risiko zu bestimmen und die angemessenen technischen und organisatorischen Massnahmen festzulegen. Es ist wichtig zu verstehen, dass diese Massnahmen zukünftig pro Prozess festgelegt werden müssen. Um nachweisen zu können, dass

RÉSUMÉ

Le temps est venu de s'adapter

Loi révisée sur la protection des données

La Loi révisée sur la protection des données, qui entrera probablement en vigueur en 2022, contraint les responsables au sein des entreprises à prendre des mesures techniques et organisationnelles qui correspondent à l'état de la technique, au type de traitement des données et à son ampleur, ainsi qu'au risque pour la personne concernée.

Pour qui n'implémente pas les mesures techniques et organisationnelles minimales (que le Conseil fédéral doit encore définir par voie d'ordonnance), l'amende, sur plainte, peut atteindre 250 000 CHF. Cette peine encourue concerne en premier lieu les personnes à la tête de l'organisation en question ; dans les sociétés anonymes, il s'agit donc en particulier des membres du conseil d'administration, et éventuellement des membres de la direction.

Il est recommandé de s'atteler dès à présent à évaluer les risques et à leur attribuer les mesures techniques et organisationnelles appropriées. En effet, leur implémentation puis la vérification de leur efficacité peuvent prendre un certain temps. Par ailleurs, tout donneur d'ordre qui, à l'avenir, conclura un contrat avec un sous-traitant devra engager ce dernier à respecter les mesures définies. À défaut de s'en charger dès maintenant, les entreprises se verront contraintes de renégocier tous les contrats au moment de l'entrée en vigueur de la Loi révisée sur la protection des données, se compliquant alors inutilement la vie (qui plus est, au prix fort). MR

man dieser Pflicht nachgekommen ist, müssen die Risikoeinschätzung und die Festlegung der entsprechenden Massnahmen dokumentiert werden. Und was das Gesetz nicht ausdrücklich erwähnt, aber augenscheinlich ist: Die technischen und organisatorischen Massnahmen, die man sich auferlegt hat, sind dann auch einzuhalten.

- Diese Dokumentationspflicht mag im ersten Moment unangenehm und mühsam erscheinen. Für Organisationen ergibt sich dennoch Spielraum, der genutzt werden kann. Die Organisationen haben ein weites Ermessen bei der Festlegung des Risikos und der «Angemessenheit» ihrer Massnahmen. Die festgelegten Massnahmen dürfen zwar nicht offensichtlich ungenügend und unverhältnismässig sein, dahinter bleibt aber ein weites Ermessen.
- Das revidierte Datenschutzgesetz benutzt in Anlehnung an die europäische Gesetzgebung die Begriffe des Verantwortlichen und des Auftragsbearbeiters. Der Verantwortliche entscheidet über die Zwecke und die Mittel der Datenbearbeitung. Der Auftragsbearbeiter bearbeitet die Daten im Auftrag des Verantwortlichen. Beim Verantwortlichen könnte es sich beispielsweise um ein Elektrizitätsunternehmen handeln, das Personendaten für die Leistungserbringung und das Inkasso verwendet. Ein Auftragsverarbeiter liegt etwa vor, wenn ein Anbieter von Cloud-Lösungen diese Daten für den Verantwortlichen speichert. Mit dem revidierten Datenschutzgesetz muss neu der Verantwortliche sicherstellen, dass sein Auftragsbearbeiter die notwendigen technischen und organisatorischen Massnahmen implementiert. Neu kann sich ein Elektrizitätsunternehmen also nicht mehr darauf berufen, dass es die Aufgabe des Cloud-Anbieters sei, für die notwendigen Massnahmen zu sorgen. Vielmehr muss das Elektrizitätsunternehmen den Cloud-Anbieter als Auftragsbearbeiter vertraglich verpflichten, die notwendigen Massnahmen sicherzustellen. Dies geschieht in einem sogenannten Auftragsverarbeitungsvertrag (Data Processing Agreement – DPA).

Frühzeitiges Handeln lohnt sich

Es ist zu empfehlen, sich bereits jetzt mit der Risikobewertung und der Zuordnung der technischen und organisatorischen Massnahmen zu beschäftigen. Denn die Implementierung beziehungsweise Überprüfung der Wirksamkeit der festgelegten Massnahmen kann einige Zeit in Anspruch nehmen. Ausserdem hat jeder Auftraggeber, der in Zukunft einen Vertrag mit einem Auftragsverarbeiter abschliesst, diesen bezüglich der festgelegten Massnahmen zu verpflichten. Wer dies nicht bereits jetzt angeht, muss bei Inkrafttreten des revidierten Datenschutzgesetzes alle Verträge nachverhandeln, womit er sich das Leben unnötig schwer (und teuer) macht.

Autoren

Klaus Krohmann ist Leiter der Rechtsberatung bei BDO Zürich.
→ BDO AG, 8031 Zürich
→ klaus.krohmann@bdo.ch

Martin Greuter ist Rechtsberater bei BDO Zürich.
→ martin.greuter@bdo.ch