DATENSCHUTZ

Neue Bestimmungen, komplexe Anwendungen

VON JAN HOLLING
Dr. Jan Holling ist Jurist und zertifizierter Datenschutzbeauftragter. Als Consultant bei der Althammer & Kill GmbH & Co. KG unterstützt er bundesweit Unternehmen in Strategiefragen, beim IT-Risikomanagement sowie bei den Themen Datenschutzrecht und Informationssicherheit.
www.althammer-kill.de

Die neue Verordnung der Europäischen Union zum Datenschutz muss künftig mit nationalem Recht in Einklang gebracht werden. Dies hat Auswirkungen auf soziale Dienste und Einrichtungen.

Seit dem 25. Mai 2017 gelten im Wechselspiel für privatwirtschaftliche soziale Unternehmungen BRD-weit das neue Bundesdatenschutzgesetz (BDSG) sowie EU-weit die Datenschutz-Grundverordnung (DSGVO oder DS-GVO).

Das Zusammenspiel dieser beiden Regelwerke ist durchaus komplex. Grundsätzlich ist der Vorrang der EU Verordnung zu beachten. Das letzte Wort hat in Zweifelsfällen der Europäische Gerichtshof, was perspektivisch erneut zu Rechtsunsicherheit führen wird. Datenschutzbeauftragte in sozialen Unternehmungen sollten daher stets zuerst in die Datenschutz-Grundverordnung und danach in das BDSG-neu schauen.

Datenschutzbeauftragter

Das neue Gesetz bleibt bei der bisherigen Regelung, welche besagt, dass ein Datenschutzbeauftragter zu bestellen ist, wenn in der Regel mindestens zehn Personen ständig mit digitaler Datenverarbeitung beschäftigt sind. Hiermit weicht der Bundesgesetzgeber ganz eindeutig von den kleinen und mittelständischen Unternehmen begünstigenden Regelungen der Datenschutz-Grundverordnung ab. Nach dem Willen des EU-Gesetzgebers hätte es für zahlreiche Unternehmen gereicht, einen Datenschutzbeauftragten erst ab 250 in Vollzeit angestellten Personen zu bestellen.

Auch für kirchliche und öffentliche soziale Unternehmungen gilt die Datenschutz-Grundverordnung mittelbar. Die Landesdatenschutzgesetze sowie die kirchlichen Gesetze zum Datenschutz müssen ebenfalls mit ihr in Konkordanz gebracht werden. Einschlägige Gesetzesvorhaben sind bereits auf dem Weg. Die entsprechenden Kirchenordnungsentwürfe sehen als Novum zum Teil auch Bußgelder vor. Auch die Datenübermittlung an und in Drittländer oder an internationale Organisationen durch kirchliche Einrichtungen soll zukünftig zulässig werden. Weiterhin bleibt es gemäß § 1 BDSG-neu bei der bisherigen Unterscheidung zwischen öffentlichen und nichtöffentlichen datenverarbeitenden Stellen. Dies wäre nach dem Telos der DSGVO nicht erforderlich gewesen.

Grundsätze der Datenverarbeitung

Die zentrale Norm ist in Zukunft Art. 5 Abs. 1 Datenschutz-Grundverordnung, welche die Rechtmäßigkeit der Speicherung von personenbezogenen Daten auf folgende sechs Säulen stellt. Daten müssen demnach

1. unter Nachweis einer rechtlichen Grundlage und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden,
2. für festgelegte und eindeutige Zwecke,
3. auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein,
4. sachlich richtig sein,
5. nur so lange gespeichert werden, wie dies erforderlich ist
6. und sicher verwahrt werden, indem technischer Schutz vor unbefugtem Datenabfluss und vor unbeabsichtigter Zerstörung gewährleistet wird.

Die datenspeichernde soziale Einrichtung ist für die Einhaltung dieser Grundsätze verantwortlich und muss deren Einhaltung nachweisen können.

DOI: 10.5771/1613-0707-2018-2-30

Sie ist folglich rechenschaftspflichtig, gegenüber Behörden und Betroffenen, insbesondere was die Rechtsgrundlage der Datenspeicherung angeht. Diese kann sich inter alia aus einem Gesetz (DSGVO, SGB etc.) oder einem Vertrag (z. B. Arbeitsvertrag, Heimvertrag etc.) ergeben.

Selbstanzeige

Gemäß Art. 33 DS-GVO muss im Falle einer Verletzung des Schutzes personenbezogener Daten eine soziale Einrichtung binnen 72 Stunden, nachdem der »Data-Breach« bekannt wurde, der zuständigen Aufsichtsbehörde den Vorfall melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der Betroffenen führt. Eine Selbstanzeige wird gerade bei einem Verlust beispielsweise von Gesundheitsdaten in der Regel nötig sein, da dann grundsätzlich ein schwerer Eingriff in das Persönlichkeitsrecht vorliegt. Erfolgt die Meldung an die Aufsichtsbehörde nicht innerhalb 72 Stunden, so ist ihr zudem eine Begründung für die Verzögerung beizufügen.

Datenschutzanfragen

Auch hier wurde im Wege der ausführlichen §§ 32-37 BDSG-neu versucht, viel vom bestehenden und bewährten Datenschutzrecht beizubehalten. Dennoch sind sie in Verbindung mit Art. 14 und 15 DSGVO zu verstehen, welche neue Auskunftspflichten für Unternehmen positivieren. So haben Kunden, Klienten und Betroffene ein Recht auf Auskunft an das datenspeichernde Unternehmen.

Neue Dokumentationspflichten

Ein Novum ist die Datenschutz-Folgeabschätzung (DSFA); sie ähnelt der aus dem momentan gültigen Bundesdatenschutzgesetz bekannten Vorabkontrolle und besteht aus mindestens vier Teilen, welche entsprechend dokumentiert werden müssen: (1) Zunächst ist eine systematische Beschreibung der Art der Speicherung und Erhebung der Gesundheitsdaten zu erstellen. (2) In einem weiteren Schritt ist die Notwendigkeit und die Verhältnismäßigkeit der Speicherung und Erhebung der Daten zu dokumentieren. (3) Sodann hat eine Bewertung der Risiken für die Beeinträchtigung des Rechts auf informationelle Selbstbestimmung der Klienten, etwa im Falle einer Datenpanne oder eines Datenverlustes, zu erfolgen. (4) Schließlich sollten die zur Bewältigung der Risiken der Beeinträchtigung der Privatsphäre (hoffentlich) getroffenen Maßnahmen verschriftlicht werden.

Sanktionen

Auch in diesem Feld war der bundesdeutsche Gesetzgeber fleißig und geht über das von der Datenschutz-Grundverordnung geforderte Maß hinaus. Zusätzlich zu den »happigen« Bußgeldern der DSGVO, mit bis zu 20 Millionen Euro beziehungsweise 4 % vom Vorjahresumsatz, je nachdem welcher Betrag höher ist, sind flankierend Freiheitsstrafen vorgesehen. Die Datenschutzbehörden sind nach der DSGVO mit weitreichenden Kontrollbefugnissen ausgestattet. Die Behörden dürfen als ultima ratio eine Einrichtung besuchen (Ortstermin) und für ihre Ermittlungen ungehindert die gesamte interne Einrichtungs-IT verwenden, um etwaige Datenschutzverstöße feststellen zu können.

Fazit

Die Datenschutz-Grundverordnung muss zukünftig stets im Kontext des BDSG-neu gelesen werden. Viele Paragraphen des BDSG-neu sind jedoch für privatwirtschaftliche soziale Unternehmungen irrelevant. So können Rechtsanwender häufig die Paragraphen des dritten Teils, § 45 bis § 84 und damit fast die Hälfte des ganzen Gesetzes ignorieren. Soziale Unternehmungen sollten zusammengefasst folgende sieben »ToDos« beachten:

1. Einstimmung auf die verschärften Regelungen zum Umgang mit Bewohnerdatenpannen (Pflicht zur Selbstanzeige innerhalb von 72 Stunden),
2. die Verschriftlichung einer so genannten Datenschutz-Folgeabschätzung bei der (digitalen) Dokumentation von Daten und dabei
3. die Beachtung der erweiternden des Begriffs der Gesundheitsdaten beziehungsweise medizinischen Daten sowie die
4. »unternehmerische« Berücksichtigung der um den Faktor 67 erhöhten Bußgelder im Falle von Datenschutzverstößen (= bis zu 20 Millionen Euro).
5. Falls noch nicht erfolgt: Die umgehende Bestellung einer oder eines Beauftragten für den Datenschutz.
6. Anpassung von Verfahrensverzeichnissen, u. U. Homepage und Datenschutzvereinbarungen.
7. Last but not least müssen Betriebsvereinbarungen auf Vereinbarkeit mit dem neuen Datenschutzrecht überprüft werden. ■

Literatur

Kort: Der Beschäftigtendatenschutz gem. § 26 BDSG-neu, in: ZD 2017, 319.

Wurzberger: Anforderungen an Betriebsvereinbarungen nach der DS-GVO, in: ZD 2017, 258.

Kühling: Neues Bundesdatenschutzgesetz – Anpassungsbedarf bei Unternehmen, in: NJW 2017, 1985.

Paal/Hennemann: Big Data im Recht, in: NJW 2017, 1697.

von Schenck/Mueller-Stöfen: Die Datenschutz-Grundverordnung: Auswirkungen in der Praxis, in: GWR 2017, 171.

Link zum BDSG n.F.: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.ppdf%27%5D__1499333759189.