Datenschutz

Neue Pflichten

[28.10.2016] Die EU-Datenschutz-Grundverordnung geht mit neuen Pflichten und höheren technischen und organisatorischen Anforderungen für die Kommunen und deren Rechenzentren einher. Bei Verstößen ist mit hohen Bußgeldern zu rechnen.

Die Organe der EU haben sich im Dezember 2015 auf eine EU-Datenschutz-Grundverordnung (DSGVO) geeinigt. Nach einer Übergangszeit wird sie ab dem 25. Mai 2018 in sämtlichen Mitgliedstaaten unmittelbar gelten. Nationale Datenschutzgesetze wie das deutsche Bundesdatenschutzgesetz (BDSG) werden dann in der jetzt geltenden Fassung nicht mehr anzuwenden sein. Die DSGVO enthält allerdings zahlreiche Öffnungsklauseln, aufgrund derer die Mitgliedstaaten lückenausfüllende nationale Regelungen treffen. Ein BDSG-Anpassungsgesetz ist in Vorbereitung. Deutschland wird ein Mitglied in den neu geschaffenen Europäischen Datenschutzausschuss entsenden, der die Verordnung auszulegen, strittige Fragen zu klären und für ein höheres Maß an Rechtssicherheit bei der Anwendung der DSGVO zu sorgen hat. Alle Verantwortlichen müssen sich mit der neuen Datenschutz-Grundverordnung alsbald vertraut machen. Verstoßen eine Kommune oder ihr Rechenzentrumsbetreiber gegen die DSGVO, weil etwa die strengen Erlaubnistatbestände für die Verarbeitung personenbezogener Daten, die Anforderungen an Einwilligungserklärungen oder Transparenzpflichten missachtet werden, so können Bußgelder in Höhe von bis zu 20 Millionen Euro verhängt werden. Auch wenn aufgrund der mangelnden Bestimmtheit einiger Bußgeldtatbestände Zweifel an ihrer Wirksamkeit bestehen, so ist der Abschreckungseffekt doch vorhanden.

Verantwortliche haften zivilrechtlich

Hinzu kommt, dass Verantwortliche und Auftragsverarbeiter gegenüber den von einem Verstoß Betroffenen gesamtschuldnerisch auf Ersatz der durch den Rechtsverstoß entstandenen Schaden zivilrechtlich haften (Artikel 82 Absatz 1 DSGVO). Sowohl gegen Rechenzentrumskunden (Kommunen) als auch gegen beteiligte Auftragsverarbeiter (Rechenzentren und Unterauftragnehmer), kann ein Ersatz des immateriellen oder materiellen Schadens geltend gemacht werden. Bei diesem Anspruch handelt es sich um eine Verschuldenshaftung wegen unerlaubter Handlung mit Beweislastumkehr. Der für den Datenschutzverstoß Verantwortliche kann sich von dem Vorwurf des Verschuldens entlasten, wenn ihm der Beweis gelingt, dass er weder vorsätzlich noch fahrlässig gehandelt hat, er also „in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist“ (Abs. 3). Der Auftragsverarbeiter haftet, „wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat“ (Abs. 2 Satz 2). Faktisch bedeutet das, dass der wirtschaftlich Stärkste als Gesamtschuldner in Höhe der gesamten Schadenssumme in Anspruch genommen werden kann. Dieser müsste nachweisen, dass der Rechtsverstoß von ihm nicht schuldhaft herbeigeführt wurde. Gelingt ihm das nicht, kann er nur noch im Innenverhältnis von den anderen Beteiligten eine Aufteilung der Haftungssumme verlangen. Welche Auswirkungen diese Perspektive auf heutige Outsourcing-Modelle hat, ist (noch) nicht abzusehen.

Kommunale Rechenzentren sind gefordert

Mit der Geltung der Datenschutz-Grundverordnung entstehen noch stärker als bisher reale Risiken für Unternehmen und Kommunen. Kommunale Rechenzentren sind daher gefordert, zeitnah ein Informations- und Dokumentationssystem aufzubauen. Wo das noch nicht geschehen ist, müssen sie mit ihren kommunalen Kunden neue Auftragsverarbeitungsverträge abschließen. Bestehende Verträge sind auf den Prüfstand zu stellen und auf ihre DSGVO-Konformität hin zu prüfen. Zudem ist wegen der Regelungen in Art. 44 ff. DSGVO nicht nur zu untersuchen, ob zu jeder Leistungsbeziehung zu einem Auftragsverarbeiter auch entsprechende DSGVO-konforme Verträge vorliegen, sondern auch, ob Auftragsverarbeiter die geforderten technischen und organisatorischen Maßnahmen treffen (Art. 28), Verzeichnisse von Verarbeitungstätigkeiten vorliegen (Art. 30), Vorkehrungen für eine datenschutzfreundliche Technikgestaltung getroffen wurden (Datenschutz durch Technikgestaltung, Art. 25; Gewährleistung der Sicherheit, Art. 32; Datenschutzfolgenabschätzung, Art. 35) und ob Daten in Drittstaaten transferiert werden, was dann weitere Maßnahmen erfordern würde. Darüber hinaus sollten die kommunalen Rechenzentren erwägen, in laufenden und zukünftigen Ausschreibungen entsprechende Zertifikate gemäß Art. 28 Abs. 5, 42 DSGVO einzufordern.

Anpassungsprozess jetzt beginnen

Erweisen sich Lieferanten von Rechenleistungen als ungeeignet, die hohen Anforderungen der EU-Datenschutz-Grundverordnung zu erfüllen, müssen neue Partner ausgewählt oder die Dienstleistungen neu ausgeschrieben und entsprechende – zumeist zeitraubende und anspruchsvolle – Migrationsprojekte begonnen werden. Des Weiteren müssen alle an der Datenverarbeitung Beteiligten damit beginnen, entsprechende Prozesse zu etablieren, um sicherzustellen, dass sie die Anforderungen der DSGVO zukünftig jederzeit einhalten. Zusätzlich müssen die kommunalen Rechenzentren prüfen, ob sie die gesteigerten technischen und organisatorischen Anforderungen – gemäß Stand der Technik – erfüllen. Sollte dies nicht der Fall sein, sind Maßnahmen einzuleiten, um das Datenschutzniveau zu steigern. Es kann davon ausgegangen werden, dass die deutschen Datenschutzanpassungsgesetze aufgrund der Öffnungsklausel in Art. 37 Abs. 4 DSGVO auch künftig betriebliche und behördliche Datenschutzbeauftragte vorsehen, die an den Maßnahmen beteiligt werden sollten. Es empfiehlt sich, mit der Bearbeitung aller genannten Aufgaben bereits jetzt zu beginnen. Zumal die Ressourcen, die sich in den Unternehmen mit Datenschutz beschäftigen, eher begrenzt sind und Datenschutzbeauftragte ihre Tätigkeit häufig neben ihren Hauptaufgaben im Tagesgeschäft ausführen. Als beratende Aufgabenträger sollten sie dazu drängen, mit den Anpassungsprozessen jetzt zu beginnen und daran auch mitwirken. Die Aufgaben sind vielfältig und können unabhängig von den derzeit noch laufenden Gesetzgebungsverfahren für ein BDSG-Anpassungsgesetz angegangen werden, um dann am 25. Mai 2018 den Anforderungen vollumfänglich gerecht zu werden.

()

Dieser Beitrag ist im Titel der November-Ausgabe von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Datenschutz, EU-Datenschutz-Grundverordnung (DSGVO), Europa