Beschluss der Fachkommission Digitalisierung und Daten 17. Mai 2019

Änderung des § 38 BDSG „Datenschutzbeauftragte nichtöffentlicher Stellen“:

(1) [1]Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit **dort in der Regel mindestens 20 Beschäftigte tätig sind**. [2]Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

(2) § 6 Absatz 4, 5 Satz 2 und Absatz 6 finden Anwendung, § 6 Absatz 4 jedoch nur, wenn die Benennung einer oder eines Datenschutzbeauftragten verpflichtend ist.

Begründung:

Satz 1 entspricht inhaltlich im Wesentlichen der bisherigen Regelung des § 38 Absatz 1 Satz 1 BDSG, verzichtet aber auf die missverständliche und vom Rechtsanwender selbstständig

auszulegenden Begrifflichkeit der ständigen Verarbeitung personenbezogener Daten. Vereine und Kleinunternehmen werden durch diese gesetzgeberische Klarstellung eindeutiger von der Bestellpflicht ausgenommen. Durch das Abstellen auf den Beschäftigtenbegriff werden dadurch nun ausdrücklich Vereine und Institutionen, deren Arbeit vorrangig ehrenamtlich erfolgt, ausgenommen.

Beschluss der Fachkommission Digitalisierung und Daten 17. Mai 2019

Zum aktuellen Gesetzentwurf zum IT-Sicherheitsgesetz 2.0 und den darin enthaltenen Vorschlägen zur Strafbarkeit von Hacking, Doxxing und Straftaten im und unter Nutzung des Darknet empfiehlt die Fachkommission Informationsrecht im BACDJ Folgendes:

Alle gesellschaftlichen Gruppen sind auf funktionierende Informationstechnik und eine sichere Infrastruktur angewiesen. Anfang des Jahres wurde der Öffentlichkeit deutlich vor

Augen geführt, dass es Menschen gibt, die Schwachstellen in der digitalen Infrastruktur ausnutzen und mit Hacking- und Doxxing-Angriffen anderen Menschen schaden wollen.

Es ist die Aufgabe des Staates, ein deutliches Zeichen zu setzen, dass solche Angriffe nicht hingenommen werden. Es muss gewährleistet sein, dass Hacking und Doxxing sowie andere Straftaten unter Nutzung des Internet strafrechtlich konsequent verfolgt werden können. Daher begrüßt der BACDJ den Vorschlag des Bundesministeriums des Innern für Bau und Heimat, im IT-Sicherheitsgesetz 2.0 neue strafrechtliche Normen zum Schutz der Bürgerinnen und Bürger im Internet zu schaffen und vorhandene Bestimmungen zu schärfen und rechtsdogmatisch konsistent anzupassen.